Kanton Zürich
Regierungsrat

Kantonale Cybersicherheits-strategie – Organisation und Umsetzung

4. Mai 2022

Inhalt

1. Allgemeine Bestimmungen

Mit dem vorliegenden Dokument werden die Inhalte und die Umsetzung der «Cybersicherheitsstrategie» im Kanton Zürich aufgezeigt. Es beschreibt die dafür notwendigen Schlüsselaufgaben, die zu erbringenden Leistungen sowie die Zuständigkeiten für den Umgang mit Cyberrisiken. Viele der Aufgaben sind gemeinsam anzugehen; die Zusammenarbeit mit Partnern soll zur Stärke des Kantons beitragen, um den Ansprüchen der Verwaltung, der Bevölkerung und der Wirtschaft gerecht zu werden. Diese Zusammenarbeit umfasst insbesondere den Bund und andere Kantone; der Kanton Zürich integriert deren Entwicklungen und gestaltet sie mit.

Das Thema des verwaltungsweiten Kontinuitätsmanagements (Business Continuity Management [BCM]) ist nicht Teil der Cybersicherheitsstrategie. Diese übergeordnete Sicherstellung des Verwaltungsbetriebs wird durch einen separaten Auftrag weiterverfolgt (vgl. RRB Nr. 172/2021).

2. Elemente der Strategie

Die wesentlichen Bestandteile der Strategie (Vision, Ziele, Grundsätze und Handlungsfelder) sind in der folgenden Abbildung dargestellt:

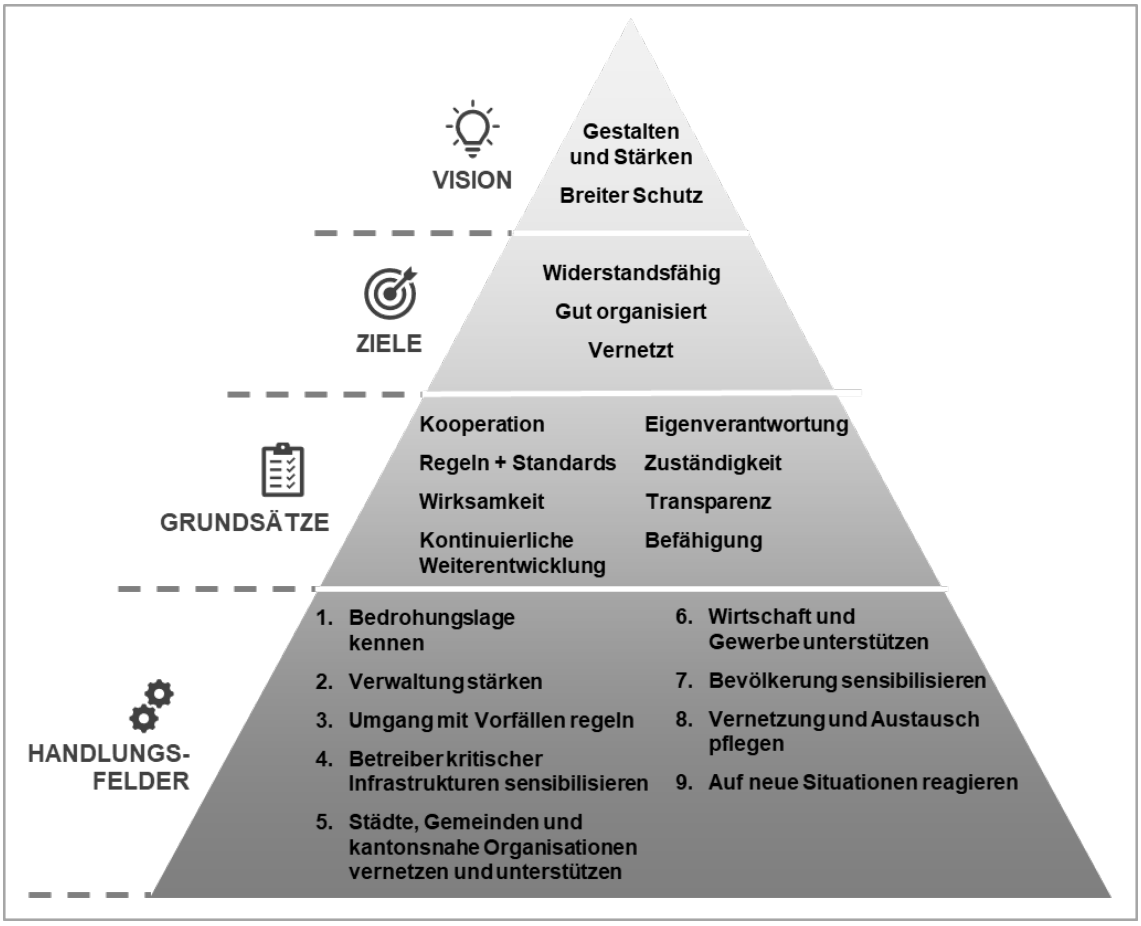


Abbildung 1: Elemente der kantonalen Cybersicherheitsstrategie

3. Handlungsfelder und Aufgaben

Um die in der kantonalen Cybersicherheitsstrategie beschriebenen Ziele umzusetzen, müssen in den Handlungsfeldern verschiedene Aufgaben erfüllt werden. Dafür werden entweder neue Projekte gestartet oder die Aufgaben werden durch bereits bestehende Projekte abgedeckt. Langfristige Aufgaben können entweder in bestehende Linienfunktion integriert werden oder es werden neue Stellen geschaffen.

Die Abbildung 2 zeigt die Zuordnung der Aufgaben in den neun Handlungsfeldern zu den verschiedenen Organisationselementen der zukünftigen Cybersicherheitsorganisation:

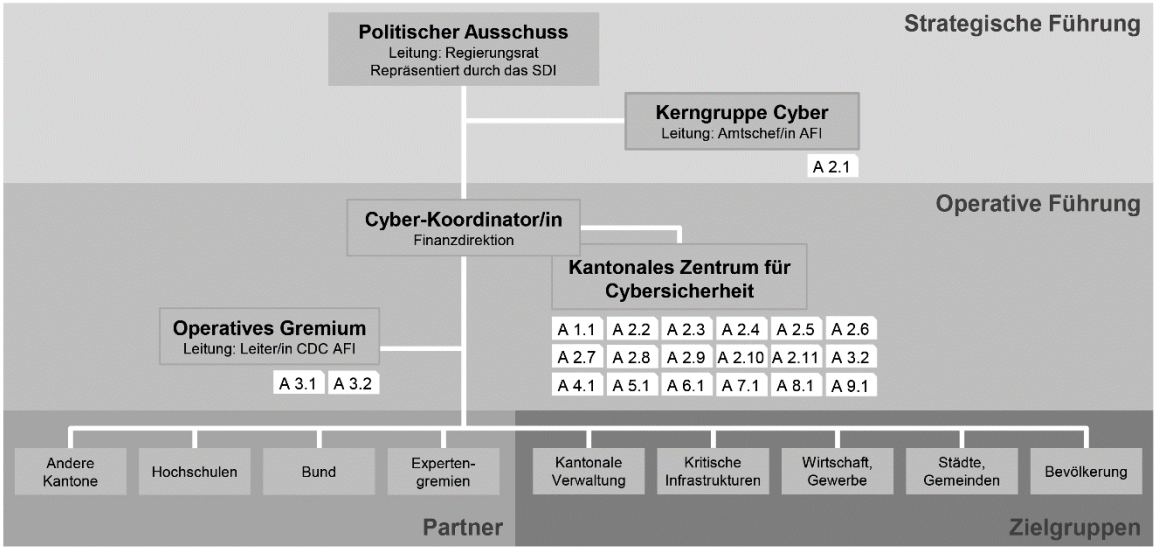


Abbildung 2: Zuständigkeiten der Organisationseinheiten für die nachfolgend beschriebenen Aufgaben. Zu beachten ist, dass für einen Teil von Aufgabe 3.2 das Kantonale Zentrum für Cybersicherheit und für einen anderen das Operative Gremium zuständig ist.

Dabei entsprechen die Bezeichnungen in den weissen Kästchen den Aufgaben wie sie in den nachfolgenden Kapiteln 3.1 bis 3.9 ausgeführt werden. Pro Aufgabe sind jeweils ein Kurzbeschrieb, die erwarteten Ergebnisse, Zielgruppen und Zuständigkeiten sowie eine grobe Schätzung des Aufwands (Personentage, Sachkosten) angegeben. Grau hinterlegte Aufwände und Kosten sind durch neu zu schaffende interne Stellen oder bereits bewilligte Mittel abgedeckt.

3.1 Handlungsfeld 1: Bedrohungslage kennen

A 1.1	Bedrohungslagebild
Beschreibung	Die Cyber-Koordinatorin oder der Cyber-Koordinator oder die von ihr oder ihm angewiesenen Stellen kennen Plattformen, Architekturen, Systeme, Applikationen, die Bedrohungen, die relevanten aktuellen Entwicklungen und Schwachstellen. Sie führen das Bedrohungslagebild nach und führen spezifische Gefährdungsanalysen durch. Diese Anstrengungen unterstützen bei präventiven Massnahmen, der Erkennung sowie Abwehr von Cyberangriffen.
Ergebnisse, Dienstleistungen	– Bedrohungslagebild: Frage geklärt, ob ein System zur Nachführung des Bedrohungslagebilds beschafft oder entwickelt wird. System implementiert und operativ einsatzfähig. – Bei Bedarf (Basis: Bedrohungslagebild, spezifische Inputs) Bedrohungsanalyse ausgelöst, eingefordert und ausgewertet.
Zielgruppe(n)	– Kantonale Verwaltung – Weitere Organe des Kantons Zürich – Kritische Infrastrukturen – Weitere: später
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung	– Kantonales Zentrum für Cybersicherheit – Abteilung Cybercrime, Kapo – Kapo-IT – Staatsanwaltschaft – Externe MSSP des AFI sowie der Kapo
Meilensteine	Bis Q2/23 Aufbau Ab Q3/23 Regelmässiger Betrieb
Aufwand Initialisierung	– Rund 50 PT / Fr. 50 000[1] – Fr. 100 000 Sachaufwand (Lizenzkosten, Konfiguration)
Aufwand laufender Betrieb	– Rund 50 PT / Fr. 50 000/Jahr – Fr. 25 000 (Wartung und Lizenzkosten)
Bemerkungen	Für das Bedrohungslagebild werden Daten aus allen zu Verfügung stehenden Quellen beigezogen. Dies beinhaltet unter anderem Bedrohungsinformationen, aktuelle Sicherheitslücken, versuchte Angriffe auf die Zentralverwaltung

[1] Grau hinterlegte Aufwände und Kosten sind durch neu zu schaffende interne Stellen oder bereits bewilligte Mittel abgedeckt.

A 1.1	Bedrohungslagebild
	sowie auf die Zielgruppen. Hier ist eine Zusammenarbeit mit dem NCSC und dem SECO (Bedrohungsradar) anzustreben; Synergien sind zu nutzen. Zu klären ist, ob eine Früherkennung von Trends und Technologien erfolgen soll (zusammen mit Hochschulen und Forschung).

3.2 Handlungsfeld 2: Verwaltung stärken

A 2.1	Überprüfung und Weiterentwicklung Cybersicherheits-strategie einschliesslich Umsetzungsdokument
Beschreibung	Die Cybersicherheitsstrategie umfasst ein Strategiedokument und ein Umsetzungsdokument. Das Umsetzungsdokument wird regelmässig überprüft und weiterentwickelt.
Ergebnisse, Dienstleistungen	– Regelmässige Überprüfung und Anpassung des Umsetzungsdokuments und Aktualisierung der Projekte – Überprüfung und Weiterentwicklung der Cybersicherheitsstrategie bei Bedarf.
Zielgruppe(n)	– Regierungsrat – Kantonale Verwaltung
Zuständigkeit	Kerngruppe Cyber
Mitwirkung / Externer Partner	– Fallweise externe Auftragnehmende – Kantonales Zentrum für Cybersicherheit – Expertenpool Informationssicherheit – FAGIS – Kapo-IT
Meilensteine	– Überprüfung und Weiterentwicklung: halbjährlich oder bei Bedarf – Parallel dazu Überprüfung der Organisationsstruktur und der Prozesse – Anschliessende Aktualisierung des Umsetzungsdokuments und der Projekte
Aufwand Initialisierung	
Aufwand laufender Betrieb	Rund 15 PT / Fr. 25 000/Jahr
Bemerkungen	Halbjährliche Überprüfung des Umsetzungsdokuments mit Blick nach vorne: – Monate 1 bis 6 Monate detailliert geplant – Monate 7 bis 12 grob geplant – Monate 13 bis 18 als Ausblick festgehalten

A 2.2	Regelwerk Informationssicherheit
Beschreibung	Das interne Regelwerk der kantonalen Verwaltung besteht aus der Allgemeinen Informationssicherheitsrichtlinie (AISR), den Besonderen Informationssicherheitsrichtlinien (BISR) sowie den Basiskonfigurationen. Die Basiskonfigurationen enthalten konkrete Empfehlungen zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Massnahmen zur Umsetzung der allgemein gehaltenen Richtlinien. Das interne Regelwerk der kantonalen Verwaltung ist aktuell zu halten und insbesondere bei neuen Bedrohungen sowie Technologien anzupassen. Die Umsetzung der internen Richtlinien in den Direktionen und der Staatskanzlei ist zu standardisieren, zu priorisieren und zu messen.
Ergebnisse, Dienstleistungen	**Initialisierung** – Die internen Interessengruppen für das Regelwerk sind identifiziert (z.B. Steuerungsgremien, Technologieboards). – Die Methodik für die Umsetzung, Verwaltung und Überwachung der AISR, BISR und Basiskonfigurationen ist definiert. **Betrieb** – Erarbeitung von konkreten Basiskonfigurationen für die Umsetzung der AISR und BISR – Weiterentwicklung der internen Richtlinien aufgrund neuer Bedrohungslagen oder Technologien – Anpassung der konkreten Basiskonfiguration aufgrund neuer Bedrohungslagen oder Technologien
Zielgruppe(n)	Kantonale Verwaltung
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung / Externer Partner	– Kantonales Zentrum für Cybersicherheit – Expertenpool Informationssicherheit – FAGIS – Kapo-IT
Meilensteine	Bis Q3/22 Die internen Interessengruppen und die Methodik sind definiert. Bis Q4/22 Die Basiskonfigurationen für die Bedrohung Ransomware sind erarbeitet. Ab Q4/22 Rollout der Basiskonfiguration für die Bedrohung Ransomware in den Direktionen und der Staatskanzlei

A 2.2	Regelwerk Informationssicherheit
	Ab Q1/23 Überführung in Regelbetrieb mit neuen Basiskonfiguration in Abhängigkeit von der aktuellen Bedrohungslage
Aufwand Initialisierung	Abgedeckt durch RRB Nr. 1193/2020
Aufwand laufender Betrieb	– Bis 2023: Abgedeckt durch RRB Nr. 1193/2020 – Ab 2024: Fr. 100 000 jährlich für Weiterentwicklung des internen Regelwerks sowie für die Erstellung neuer Basiskonfigurationen
Bemerkungen	

A 2.3	Risikomanagement Informationssicherheit
Beschreibung	Etablierung eines integrierten, technisch gestützten Risikomanagements Informationssicherheit, mit dem die kantonale Verwaltung Bedrohungen und Schwächen im Bereich der Informationssicherheit frühzeitig und dynamisch erkennt und über die Einschätzung zu entsprechenden Auswirkungen die Massnahmen und Investitionen besser steuert. Der Umgang mit Risiken ist mit dem integralen Risikomanagement sowie dem internen Kontrollsystem (IKS) abzugleichen. Synergien sind zu nutzen, z.B. im Bereich BCM.
Ergebnisse, Dienstleistungen	**Etablierung einer integrierten Risikomanagementfunktion im Bereich Informationssicherheit** – Festlegung der Organisation für die Risikolenkung sowie der Methoden und Instrumente – Erarbeitung der Anforderungen für die technische Unterstützung – Unterstützung bei der Selektion und Implementierung eines Tools zur Unterstützung des Risikomanagements **Governance Risikomanagement** – Entwicklung der Information Risk Governance für die gesamte Verwaltung zur Steuerung der dazugehörigen Risiken und Massnahmen – Einheitliche Begrifflichkeit und Klassifikation von Systemrelevanz und Kritikalitätsgrad – Asset-Management (Inventurkontrolle) – Bewertung und Einschätzung der Cybersicherheit nach Geschäftsprozessen der Ämter – Risiko- und Schwachstellenkatalog einschliesslich Supply-Chain-Risiken (Hersteller, Lieferanten, Betreiber) – Monitoring des Lebenszyklus der Schutzobjekte wie z.B. einer Applikation oder eines Services (Überarbeitung Schutzbedarfsanalyse usw.). **Ausbau zur Abdeckung aller Bereiche des Risikomanagements Informationssicherheit für alle Direktionen und die Staatskanzlei** – Sukzessiver Aufbau eines Teams – Begleitung bei der sukzessiven Ausweitung und Dynamisierung der Lösung durch Anbindung zusätzlicher Quellen
Zielgruppe(n)	Kantonale Verwaltung
Zuständigkeit	Cyber-Koordinator/in

A 2.3	Risikomanagement Informationssicherheit
Mitwirkung / Externer Partner	– Kantonales Zentrum für Cybersicherheit – Expertenpool Informationssicherheit – FAGIS – Softwareanbietende – Kapo-IT
Meilensteine	Bis Q1/23 Etablierung der Funktion, Inbetriebnahme einer Basislösung für die Geschäftsprozesse des AFI (im Sinne eines Minimum Viable Products bzw. einer ersten minimalen, aber funktionsfähigen Lösung) Bis Q3/23 Abdeckung von 50% in der kantonalen Verwaltung Bis Q2/24 Abschluss mit kompletter Abdeckung in den Direktionen und der Staatskanzlei
Aufwand Initialisierung	Rund Fr. 350 000 (Implementierungskosten für die Software)
Aufwand laufender Betrieb	– 1 FTE (Leiter/in kantonales Risikomanagement Informationssicherheit) – 3 FTE (Risiko-Analystinnen/-Analysten) – Lizenzkosten: rund Fr. 250 000/Jahr – Weiterentwicklungskosten für die Softwarelösung: rund Fr. 50 000/Jahr
Bemerkungen	Eine separate Beschaffung für die Software wird notwendig werden (Tool für Information Risk Management).

A 2.4	Kantonale Sicherheitskultur
Beschreibung	Die im Konzept Sicherheitskultur (TreeSolution GmbH, Version 1.1, März 2021) identifizierten Massnahmen zur Stärkung der Sicherheitskultur werden umgesetzt.
Ergebnisse, Dienstleistungen	– Aufbau und Durchführung Ausbildungsprogramm für Informationssicherheit-, IT- und Prozessverantwortliche (Konzept und im Anschluss externe Schulungsdienstleister) – Aufbau und Betrieb Security-Awareness-Plattform mit E-Learning für Mitarbeitende und Vorgesetzte (gegebenfalls Learning-Management-Plattform), Kampagnenmaterial für Security Awareness – Intranetportal Informationssicherheit warten – Spezifizierter Umgang mit sicherheitsrelevanten Informationen festlegen – Kommunikationsplan für Cyber-Koordinator/in und ISID erstellen
Zielgruppe(n)	Kantonale Verwaltung
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung / Externer Partner	– Kantonales Zentrum für Cybersicherheit – Externe Unterstützung für konzeptionelle Arbeiten – Addon (extern, Ausbildung, Kurse) – Kapo
Meilensteine	Ab Q3/22 Weiterer Ausbau, Wartung und Aktualisierungen
Aufwand Initialisierung	
Aufwand laufender Betrieb	– Fr. 50 000/Jahr (Wartung, Klassifizierungsrichtlinien, Kommunikation) – Rund Fr. 100 000/Jahr Lizenzkosten (Security-Awareness-Plattform, Trainingsmodul für Phishing) – 1 FTE Security-Awareness-Spezialist/in – Rund Fr. 100 000/Jahr Ausbildungsprogramm durchführen – Rund Fr. 50 000/Jahr konzeptionelle Weiterentwicklung
Bemerkungen	

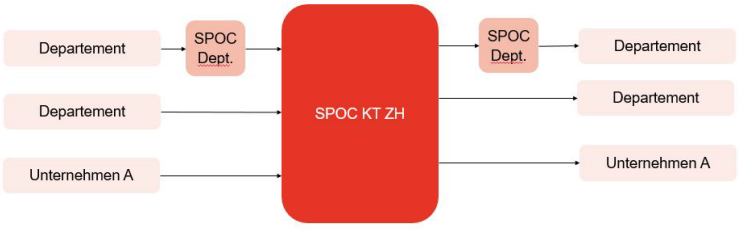
A 2.5	Audits im Bereich Informationssicherheit
Beschreibung	Mit Audits sollen Nichtkonformitäten bzw. Handlungsbedarf innerhalb der kantonalen Verwaltung im Bereich Informationssicherheit erkannt werden und diesen nachhaltig entgegengewirkt werden. Die Leiterin oder der Leiter internes Audit führt im Auftrag der Kerngruppe Cyber Überprüfungen im Bereich Informationssicherheit durch. Sie oder er plant die jährlichen Überprüfungen im Bereich Informationssicherheit, führt selbstständig Audits durch, erstellt Auditberichte und leitet Handlungsempfehlungen ab.
Ergebnisse, Dienstleistungen	– Jahresplanung für Audits im Bereich Informationssicherheit – Audit- und Abweichungsberichte – Massnahmenplan einschliesslich Nachverfolgung
Zielgruppe(n)	Kantonale Verwaltung
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung / Externer Partner	– Kantonales Zentrum für Cybersicherheit – Expertenpool Informationssicherheit – FAGIS – Penetration-Testing-Unternehmen
Meilensteine	Bis Q3/22 Ausschreibung der Stelle «Leiter/in internes Audit» Bis Q4/22 Auditprogramm und Auditplan für die Zentralverwaltung 2023 Bis Q2/23 Auditprogramm und Auditplan für die Zentralverwaltung 2024
Aufwand Initialisierung	
Aufwand laufender Betrieb	– 1 FTE (Leiter/in interne Audit-Funktion) – Rund Fr. 100 000/Jahr für risikobasierte Durchführung von Audits in den Direktionen und in der Staatskanzlei – Rund Fr. 100 000/Jahr für Audits der Grundversorgung im Amt für Informatik – Rund Fr. 100 000/Jahr für Audits von ZHservices – Rund Fr. 50 000/Jahr für Audits der Informationssicherheit (kantonales ISMS, ISMS in den Direktionen und der Staatskanzlei)
Bemerkungen	Die Auditfunktion in der 2nd Line ist aufgrund der fehlenden internen Revision neu aufzubauen. Die Auditplanung erfolgt in Abstimmung mit anderen Behörden mit einer Kontrollfunktion im Kanton Zürich, z.B. der Finanzkontrolle. Die Kerngruppe Cyber ist Auftraggeberin für das Audit des ISMS.

A 2.6	Expertenpool Informationssicherheit
Beschreibung	Verstärkung des direktionsübergreifenden Expertenpools Informationssicherheit für die Umsetzung der AISR und BISR in der Zentralverwaltung. Der Expertenpool setzt sich zusammen aus externen Partnern sowie einer zusätzlichen internen Fachexpertin oder Fachexperten für Informationssicherheit.
Ergebnisse, Dienstleistungen	Expertenpool bestehend aus internen und externen Mitgliedern
Zielgruppe(n)	Kantonale Verwaltung
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung / Externer Partner	– Kantonales Zentrum für Cybersicherheit – Gemäss RRB Nr. 811/2021 wurden fünf Unternehmen beauftragt.
Meilensteine	Bis Q3/22 Ausschreibung einer Stelle «Informationssicherheits-Expertin/-Experte» Bis Q2/24 Evaluation des Expertenpools und Vorschläge zur Weiterentwicklung
Aufwand Initialisierung	
Aufwand laufender Betrieb	1 FTE Informationssicherheits-Expertin/-Experte zur Verstärkung des bereits vorhandenen Expertenpools
Bemerkungen	Organisatorisch können die Informationssicherheits-Expertinnen und -Experten bei der Cyber-Koordinatorin oder dem der Cyber-Koordinator, im Team Informationssicherheit AFI oder in der Enterprise-Architektur angesiedelt werden.

A 2.7	Bug-Bounty-Programm
Beschreibung	Mithilfe eines Bug-Bounty-Programms können durch ethische Hacker Sicherheitslücken gefunden werden, die mit den klassischen Testmethoden verborgen bleiben (würden). Die primären Segmente für das Bug-Bounty-Programm sind die Kritischen Services und die Applikationen.
Ergebnisse, Dienstleistungen	– Vulnerability-Disclosure Policy – Governance-Policy – Metriken für das Bug-Bounty-Programm – Design und Umsetzung der Webseite – Bereitstellung einer zentralen Bug-Bounty-Plattform für das Gemeinwesen im Kanton Zürich
Zielgruppe(n)	– Kantonale Verwaltung – Zu prüfen in einer späteren Phase: Weitere Organe des Kantons Zürich
Zuständigkeit	Leiter/in Cyber Defence Center AFI
Mitwirkung / Externer Partner	Amt für Informatik
Meilensteine	Bis Q3/22 Vulnerability-Disclosure Policy und Governance, Controlling Bis Q4/22 Aufbau Bug-Bounty-Plattform Ab Q1/23 Inbetriebnahme Bug-Bounty-Plattform
Aufwand Initialisierung	Konzeptionelle Grundlagen für die Vulnerability-Disclosure Policy und das Bug-Bounty-Programm: rund Fr. 50 000
Aufwand laufender Betrieb	– Administration Vulnerability-Disclosure Policy-Programm: rund Fr. 50 000/Jahr – Lizenzkosten Bug-Bounty-Plattform: rund Fr. 75 000/Jahr – Zentraler Bug-Bounty-Pool: rund Fr. 100 000/Jahr – Weiterentwicklung, Kommunikation und Controlling: rund Fr. 100 000/Jahr

A 2.7	Bug-Bounty-Programm
Bemerkungen	Der allfällige Aufbau der Bug-Bounty-Plattform soll erst nach einem Abgleich mit dem Bund gestartet werden. Bei der Nutzung einer nationalen Plattform, die gegebenfalls durch das NCSC bereitgestellt wird, entfallen die oben aufgeführten jährlichen Betriebskosten. Erfahrungswerte von anderen Programmen zeigen, dass ein Budget von Fr. 25 000 für das Finden von Schwachstellen in einer Applikation bereitgestellt werden sollte. Das heisst, mit einem Bug-Bounty-Pool von Fr. 100 000/Jahr können mindestens vier unterschiedliche Applikationen an diesem Programm partizipieren. Die Anzahl der partizipierenden Applikationen ist nicht beschränkt, jedoch sind die Kosten durch die jeweiligen Fachverantwortlichen zu tragen, nachdem der zentrale Pool ausgeschöpft ist.

A 2.8	Identity and Access Management
Beschreibung	Weiterentwicklung des vorhandenen Identitäts- und Zugriffsmanagements als Anschlussprojekt an das IKT-Programm (Basis: IKT-Projekt 30.20 IAM). Benutzerkonten und Zugriffsberechtigungen im Netzwerk der kantonalen Verwaltung zentral bzw. nach vordefinierten Vorgaben verwalten.
Ergebnisse, Dienstleistungen	– Weiterentwicklung
Zielgruppe(n)	– Kantonale Verwaltung – Zu prüfen in einer späteren Phase: weitere Organe des Kantons Zürich
Zuständigkeit	Leiter/in Cyber Defence Center AFI
Mitwirkung / Externer Partner	– Amt für Informatik – Kapo
Meilensteine	Bis Q1/23 Projektstart Bis Q2/24 Aufbau IAM Ab Q3/24 laufender Betrieb
Aufwand Initialisierung	250 PT / Fr. 400 000 (Aufwand extern, Unterstützung Konzeption und mögliche Submission neue IAM-Plattform)
Aufwand laufender Betrieb	– 2 FTE Informationssicherheits-Expertin/-Experte «IAM» – Lizenz- und Betriebskosten IAM Plattform: rund Fr. 700 000/Jahr
Bemerkungen	

A 2.9	Security Operations Center und Cyber Defence Center
Beschreibung	Das bestehende Security Operations Center (SOC) wird zu einem Cyber Defence Center (CDC) weiterentwickelt, als Anschlussprojekt an das IKT-Programm. Das CDC übernimmt den Schutz der kantonalen IKT-Sicherheit sowie die Definition und Implementierung von Massnahmen. Synergien zum SOC der Kapo sollen geprüft und wo möglich genutzt werden.
Ergebnisse, Dienstleistungen	– Überwachung der Systeme der Grundversorgung sowie der Fach- und Kantonsapplikationen (Monitoring) – Endgeräte-Überwachung (EDR) – Definition Response-Teil – Cloud Access Security Broker (CASB) – Schwachstellenmanagement; technische Schwachstellenscans – Automatisiertes Penetration Testing – Blue- and Red-Teaming – Future-Proof Network Detection and Response (NDR)
Zielgruppe(n)	– Kantonale Verwaltung – Zu prüfen in einer späteren Phase, unter Einhaltung der rechtlichen Rahmenbedingung: – Weitere Organe des Kantons Zürich – Städte und Gemeinden des Kantons Zürich – Andere Kantone
Zuständigkeit	Leiter/in Cyber Defence Center AFI
Mitwirkung / Externer Partner	– Amt für Informatik – Kapo-IT – ISPIN AG, Bassersdorf
SPOC für die Koordination	Für die Früherkennung und Bewältigung von IT-Krisen ist es unerlässlich, dass die Betreiber und das kantonale Lagezentrum miteinander kommunizieren. 

A 2.9	Security Operations Center und Cyber Defence Center
	Konzept Die zentrale Aufgabe des Single Point of Contact (SPOC) ist die schnelle, unverfälschte und zuverlässige Weiterleitung von Informationen und die Alarmierung der Direktionen/ Unternehmen. – Ein SPOC soll grundlegende technische und organisatorische Fähigkeiten besitzen und über möglichst alle einsetzbaren Kommunikationsmittel verfügen und aufgrund der Informationen aus den Unternehmen die aktuelle IT-Sicherheitslage kennen. – Der SPOC soll während der Krisenbewältigung zusätzliche Ressourcen bereitstellen können wie zusätzliche Expertise und organisatorische Unterstützung. **Tätigkeiten** – Weiterleiten: Der SPOC leitet Informationen schnellstmöglich weiter. – Bewerten: Der SPOC bewertet die erhaltenen Informationen aufgrund seines Branchen-Knowhows und stellt die Relevanz der Informationen für die Direktionen und Unternehmen fest. – Aufbereiten: Der SPOC bereitet Informationen mit eigenen Erkenntnissen und Handlungsempfehlungen auf. – Lagefeststellung: Der SPOC beobachtet und bewertet die IT-Sicherheitslage. Durchführung: Der SPOC führt regelmässige Kommunikationstests, Notfall- und Krisenübungen durch.
Meilensteine	Bis Q4/21 Aufbau SOC Ab Q1/22 Laufender Betrieb Bis Q2/23 Aufbau Automatische Penetration-Plattform und CASB
Aufwand Initialisierung	– Fr. 765 000 ISPIN (abgedeckt durch RRB Nr. 965/2020) – 100 PT / Fr. 160 000 (Aufwand extern, Unterstützung Konzeption und mögliche Submission automatische Penetration-Plattform) – 150 PT / Fr. 240 000 (Aufwand extern, Konzeption und mögliche Submission CASB)
Aufwand laufender Betrieb	– Fr. 900 000 bis Fr. 1 300 000; ISPIN (abgedeckt durch RRB Nr. 965/2020) – 3 FTE Informationssicherheits-Expertin/-Experte «SOC / CDC / Security Incident Analyst» beim AFI – 1 FTE Informationssicherheits-Expertin/-Experte «SOC / CDC / Security Incident Analyst» bei der Kapo

A 2.9	Security Operations Center und Cyber Defence Center
	– Lizenz- und Betriebskosten Automatische Penetration-Plattform: rund Fr. 150 000/Jahr – Lizenz- und Betriebskosten CASB: rund Fr. 650 000/Jahr
Bemerkungen	Hardware (Rechenzentrum) wird durch das AFI betrieben; ISPIN liefert Dienstleistungen zugunsten des SOC des AFI. ISPIN deckt «monitor/collect» und «detect» ab. Bei «react/response/recover» liegt die Führung beim AFI, das von ISPIN unterstützt wird.

A 2.10	Public Key Infrastructure Services
Beschreibung	Ausbau der Public Key Infrastructure Services innerhalb der kantonalen Verwaltung
Ergebnisse, Dienstleistungen	– Betrieb und Ausbau der Public-Key-Infrastruktur – Zertifikate ausstellen – Validierungsdienst betreiben – Sperrlisten führen – Verzeichnisdienst betreiben – Ausbau der PKI-Services gegenüber Kunden – evtl. ergänzen: Erweiterung der PKI-Services bezüglich digitaler Unterschrift – Ausbildung Mitarbeitende – Support
Zielgruppe(n)	– Kantonale Verwaltung – Zu prüfen in einer späteren Phase: weitere Organe des Kantons Zürich – Zu prüfen in einer späteren Phase: Städte und Gemeinden
Zuständigkeit	AFI, Leiter/in CDC
Mitwirkung / Externer Partner	Amt für Informatik
Meilensteine	Bis Q1/23 Projektstart Bis Q2/24 Ausbau Public Key Infrastructure Services Ab Q3/24 laufender Betrieb
Aufwand Initialisierung	– Fr. 125 000 (Submission Werkzeug PKI-Prozess-unterstützung/Automation) – Fr. 75 000 (Externe Unterstützung prozessuale und technische Konzeption)
Aufwand laufender Betrieb	– 2 FTE Informationssicherheits-Expertin/-Experte «PKI» sowie 1st Level Support – Lizenz- und Betriebskostenkosten PKI: rund Fr. 350 000/Jahr
Bemerkungen	Werden Teile der PKI-Services an Dritte ausgelagert? Zu beachten ist, dass die Kapo auch Infrastrukturen und Plattformen des BIT und des EJPD nutzt.

A 2.11	Führen der Geschäftsstelle
Beschreibung	Zur Unterstützung der Cyber-Koordinatorin oder des Cyber-Koordinators und weiterer Stellen in den Bereichen Projektmanagement, Koordination und Kommunikation verfügt das kantonale Zentrum für Cybersicherheit über eine Geschäftsstelle.
Ergebnisse, Dienstleistungen	– Programmleitung – Projektmanagement-Office und Koordination – Kommunikation – Unterstützung bei der Klärung und Weiterentwicklung rechtlicher Rahmenbedingungen im Auftrag der Kerngruppe Cyber – Qualitätsprüfung (externe Dienstleistung)
Zielgruppe(n)	– Kantonale Verwaltung – Zu prüfen in einer späteren Phase: weitere Organe des Kantons Zürich – Zu prüfen in einer späteren Phase: Städte und Gemeinden
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung / Externer Partner	– Kantonales Zentrum für Cybersicherheit – Externer Partner für Qualitätsprüfung
Meilensteine	Bis Q4/22 Aufbau Ab Q1/23 Betrieb
Aufwand Initialisierung	
Aufwand laufender Betrieb	– Programmleitung: 1 FTE (intern, extern) – Projektmanagement-Office, Koordination, Kommunikation, rechtliche Rahmenbedingungen: 2 FTE – Qualitätsprüfung: Fr. 25 000/Jahr
Bemerkungen	Der Kanton nimmt eine Auslegeordnung zu den kantonalen rechtlichen Grundlagen, z.B. mit Bezug zu den kritischen Infrastrukturen vor; er identifiziert allfällige Lücken und klärt den Handlungsbedarf.

3.3 Handlungsfeld 3: Umgang mit Vorfällen regeln

A 3.1	Umgang mit Vorfällen regeln
Beschreibung	Das Vorgehen im Ereignisfall ist für alle Eskalationsstufen geklärt.
Ergebnisse, Dienstleistungen	– Aufgaben, Kompetenzen und Verantwortlichkeiten für den Ereignisfall sind in einem übergreifenden Vorfallbehandlungskonzept definiert und geregelt. – Mittel sind vorhanden, um auf Vorfälle und Cyberangriffe reagieren zu können. – Verwaltungseinheiten sind befähigt, Ereignisse fachlich und in der Führung selbstständig zu bewältigen, wo ordentliche Abläufe ausreichen. – Wo das Schadenausmass, der Leistungsbedarf und die zeitliche Dringlichkeit es gebieten, wird Unterstützung hinzugezogen. – Zeichnet sich ab, dass der Vorfall relevant für den Bevölkerungsschutz ist oder die Handlungsfähigkeit der Verwaltung eingeschränkt wird, ist die KFO beizuziehen. – Die Unterstützungsangebote und Schnittstellen sind bekannt; insbesondere zum AFI und zur KFO. – Die Führungsorganisation in der Verwaltungseinheit bleibt auch im Ereignis unverändert. – Die vorbereitete Krisenkommunikation erfolgt über die Direktion oder den Regierungsrat.
Zielgruppe(n)	Kantonale Verwaltung
Zuständigkeit	Operatives Gremium
Mitwirkung	– Kantonales Zentrum für Cybersicherheit – Kantonspolizei, Staatsanwaltschaft – Kantonale Führungsorganisation – Nationale Organisationseinheiten – Ausgewählte Branchen oder Stakeholder (z.B. Betreiber kritischer Infrastrukturen)
Meilensteine	Bis Q2/23 Aufbau Ab Q3/23 Umsetzung, Begleitung
Aufwand Initialisierung	
Aufwand laufender Betrieb	Offen; abhängig von Krisenübungen und Vorfällen

A 3.1	Umgang mit Vorfällen regeln
Bemerkungen	Die operative Führung wird stark bei den IKT-Verantwortlichen der Verwaltungseinheit sowie bei SOC/CDC- und CERT-Organisationen des AFI bzw. der IT-Kapo liegen. Im schweren Eskalationsfall werden sie verstärkt durch das NCSC. Weitere fachliche Unterstützung bieten neben den ISID die BCM-Verantwortlichen. Das übergeordnete BCM-Konzept ist in Arbeit. Der Umgang mit Vorfällen ist mit dem Projekt «Integrales Risikomanagement» abzugleichen. Synergien sind zu nutzen, z.B. im Bereich BCM.

A 3.2	Cyberkrisenmanagement
Beschreibung	Der Kanton erarbeitet ein Konzept zum Cyberkrisenmanagement, das auch die Durchführung von Cybersimulationsübungen (z.B. Ransomware-Angriff) enthalten soll.
Ergebnisse, Dienstleistungen	**Fertigstellung Konzept «Cyberkrisenmanagement» mit folgenden Inhalten:** – Szenarienanalyse, Vorgehenspläne – Prozessidentifikation und Optimierung – Eskalationsmatrix und Bewertungsraster – Organisation und Rollen – Ausbildungsplan, Tests, Übungen – Hilfsmittel für den Einsatz – Krisenkommunikation und Medienmanagement – Synthese und Präsentation **Durchführung von Trainings und Simulationsübungen** – Initiale Trainings – Initiale Simulationsübung – Stabsübung, Stabsrahmenübung **Übungen finden auf folgenden Ebenen statt** – Amtsintern – Regierungsrat und Verwaltung, Einbezug weiterer Organisationen – Kantonspolizei mit Städten und Gemeinden
Zielgruppe(n)	Kantonale Verwaltung
Zuständigkeit	– Erstellung Grundlagen: Cyber-Koordinator/in – Durchführung der Übungen: Operatives Gremium
Mitwirkung / Externer Partner	– Kantonales Zentrum für Cybersicherheit – Expertenpool Informationssicherheit – Kapo
Meilensteine	Bis Q4/22 Erarbeitung Cyberkrisenmanagement Ab Q1/23 Durchführung Simulationsübungen und Stabsübungen
Aufwand Initialisierung	– Rund Fr. 50 000: Fertigstellung Konzept Cyberkrisenmanagement – Rund Fr. 100 000: Kosten für die Durchführung von Trainings, Simulationsübung und Stabsübung
Aufwand laufender Betrieb	– Rund Fr. 100 000/Jahr: Weiterentwicklung Konzept Cyberkrisenmanagement und Wiederholung der Übungen alle zwei Jahre

A 3.2	Cyberkrisenmanagement
Bemerkungen	– Das Ziel soll sein, im Zwei-Jahres-Rhythmus die Trainings und Simulationen in Zusammenarbeit mit einem externen Partner zu wiederholen (gesamte Übungskosten Fr. 80 000). – Die Rechtsgrundlage für Cyberübungen ist mit dem Regierungsratsbeschluss Nr. 172/2021 vom 11. März 2021 geschaffen.

3.4 Handlungsfeld 4: Betreiber kritischer Infrastrukturen sensibilisieren

A 4.1	Betreiber kritischer Infrastrukturen unterstützen
Beschreibung	Die Verantwortung für den Schutz kritischer Infrastruktur liegt in erster Linie bei den Betreibern selbst. Der Kanton kennt seine kritischen Infrastrukturen und deren Risiken; er pflegt den Austausch mit den Betreibern.[2]
Ergebnisse, Dienstleistungen	– Liste Kritischer Infrastrukturen – Liste Kontaktpersonen bei Betreibern – Sitzungsraster mit Betreibern – Mitwirkung auf Stufe Bund geklärt (Teilnahme, inhaltliche Inputs) – Kontaktpflege mit den Betreibern kritischer Infrastrukturen im Kanton und Sensibilisierung bezüglich Cybersicherheit (z.B. Umsetzung des IKT-Minimalstandards des Bundesamtes für wirtschaftliche Landesversorgung).
Zielgruppe(n)	Kritische Infrastrukturen
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung	– Kantonales Zentrum für Cybersicherheit – Bundesamt für wirtschaftliche Landesversorgung – Expertenpool Informationssicherheit
Meilensteine	Bis Q4/23 Aufbau Ab Q1/24 Regelmässiger geplanter Austausch
Aufwand Initialisierung	Rund 15 PT / Fr. 25 000 für die Erstellung eines Konzepts zur Zusammenarbeit
Aufwand laufender Betrieb	Offen; abhängig von Massnahmen aus dem Konzept

[2] Vgl. dazu auch «Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022»; Massnahme 5.

A 4.1	Betreiber kritischer Infrastrukturen unterstützen
Bemerkungen	Der Bund hat die Führung bei der Unterstützung der kritischen Infrastrukturen (insbesondere bei den kritischen Infrastrukturen der Leistungsklasse 4 und 5); der Kanton Zürich unterstützt hier in noch zu bestimmender Form den Bund. Zu prüfen ist eine koordinierende Rolle des Kantons bei spezifischen Cyberkrisenmanagementübungen. Dazu findet ein Abgleich statt mit der WL AWA. Als weiterführende Ideen (insbesondere bei den kritischen Infrastrukturen der Leistungsklasse 3 und tiefer) sind denkbar: – Unterstützung der Betreiber von kritischen Infrastrukturen bei der Erstellung von Wiederanlaufplänen sowie Krisenmanagementplänen bei einen Cyberangriff, z.B. mit Mustervorlagen – Koordination von Cyberkrisenmanagementübungen mit Betreibern von kritischer Infrastruktur

3.5 Handlungsfeld 5: Städte, Gemeinden und kantonsnahe Organisationen vernetzen und unterstützen

A 5.1	Städte und Gemeinden unterstützen
Beschreibung	Der Kanton Zürich pflegt den Austausch mit seinen Städten und Gemeinden sowie dem Kantonsrat, den Parlamentsdiensten, den kantonalen Gerichten und Notariaten. Er fördert die Vernetzung der kantonalen und kommunalen Fachpersonen. Bei Bedarf und unter Einhaltung der rechtlichen Rahmenbedingung kann er Städte und Gemeinden mit den kantonalen Cybersicherheitsdienstleistungen unterstützen.
Ergebnisse, Dienstleistungen	– Liste von Kontaktpersonen der Städte und Gemeinden sowie des Kantonsrates, der Parlamentsdienste, der kantonalen Gerichte und Notariate führen – Sitzungsraster anlegen und regelmässige Austauschformate planen und durchführen – In Gesprächen Unterstützungsbedarf erkennen; für Vernetzung sorgen
Zielgruppe(n)	Städte und Gemeinden des Kantons Zürich sowie Kantonsrat, Parlamentsdienste, kantonale Gerichte und Notariate
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung	– Kantonales Zentrum für Cybersicherheit – Netzwerk egovpartner – Expertenpool Informationssicherheit
Meilensteine	Bis Q2/24 Aufbau Ab Q3/24 Austausch in Zielgruppe, Vernetzung
Aufwand Initialisierung	Rund 15 PT / Fr 25 000 für die Erstellung eines Konzepts zur Zusammenarbeit
Aufwand laufender Betrieb	Offen; abhängig von Massnahmen aus dem Konzept
Bemerkungen	Bei der Zusammenarbeit zwischen Städten, Gemeinden und dem Kanton werden vorhandene Strukturen gezielt genutzt, z.B. Verein Zürcher Gemeindeschreiber und Verwaltungsfachleute (Fachstelle ICT); der Austausch mit den Städten Zürich und Winterthur kann auch direkt erfolgen. Denkbare Leistungen zugunsten der Städte und Gemeinden könnten sein: – Nutzen des CDC – Zugriff auf Bug-Bounty-Plattform – Regelwerk Informationssicherheit zur Verfügung stellen – Informations- und Ausbildungsmaterial zur Verfügung stellen – Unterstützung durch Beratung und Mustervorlagen

3.6 Handlungsfeld 6: Wirtschaft und Gewerbe unterstützen

A 6.1	Wirtschaft und Gewerbe unterstützen
Beschreibung	Der Kanton pflegt den Austausch mit Wirtschaft und Gewerbe und fördert die Vernetzung in den Branchen. Er unterstützt Informationskampagnen der Wirtschaft und des Gewerbes.
Ergebnisse, Dienstleistungen	– Liste von Kontaktpersonen in Wirtschaft und Gewerbe sowie in den Verbänden führen – Sitzungsraster anlegen und regelmässige Austauschformate planen und durchführen, Bedürfnisse entgegennehmen – Hilfsmittel zur Vernetzung entwickelt – Inhalte für Informationskampagnen bereitstellen – Teilnahme an geeigneten Fachkonferenzen und Symposien – Liste von Drittfirmen im Kanton Zürich führen, die bei einem Cyberangriff unterstützen und beraten können
Zielgruppe(n)	Wirtschaft und Gewerbe
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung	– Kantonales Zentrum für Cybersicherheit – Netzwerk egovpartner – Expertenpool Informationssicherheit
Meilensteine	Bis Q2/24 Aufbau Netzwerk Ab Q3/24 Austausch in Zielgruppe
Aufwand Initialisierung	Rund 15 PT / Fr. 25 000 für die Erstellung eines Konzepts zur Zusammenarbeit
Aufwand laufender Betrieb	Offen; abhängig von Massnahmen aus dem Konzept
Bemerkungen	Abgleich mit der Standortförderung des AWA im Kanton Zürich (insbesondere Vernetzungsaktivitäten) anstreben Abgleich mit der nationalen Plattform «ITSec4KMU» (Lead: Kanton Zug) anstreben, Synergien nutzen, Unterstützung anbieten, Synergien mit Kapo insbesondere im präventiven Bereich nutzen (SKP). Prüfen, ob der Kanton auch selbst Kampagnen mit Fokus auf Wirtschaft und Gewerbe anstossen kann.

3.7 Handlungsfeld 7: Bevölkerung sensibilisieren

A 7.1	Bevölkerung sensibilisieren
Beschreibung	Der Kanton fördert die Aus- und Weiterbildung mit der Stärkung der Kompetenz «Cybersicherheit» in Schulen, Hochschulen und weiteren Bildungsangeboten und er unterstützt Informationskampagnen. Er kann auch selbst Informationskampagnen durchführen.[3]
Ergebnisse, Dienstleistungen	– Konzept zur Aus- und Weiterbildung «Cybersicherheit» auf allen Stufen des kantonalen Bildungssystems entwickeln – Inhalte für Informationskampagnen bereitstellen – Kommunikationsplan für Kampagnen entwickeln
Zielgruppe(n)	Bevölkerung
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung	– Kantonales Zentrum für Cybersicherheit – Bildungsdirektion – Hochschulen – Sicherheitsdirektion (Kapo) – Expertenpool Informationssicherheit
Meilensteine	Bis Q2/24 Aufbau Ab Q3/24 Umsetzung, Begleitung
Aufwand Initialisierung	Rund 15 PT / Fr. 25 000 für die Erstellung eines Konzepts zur Zusammenarbeit
Aufwand laufender Betrieb	Offen; abhängig von Massnahmen aus dem Konzept

[3] Vgl. dazu auch «Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022»; Massnahme 4.

A 7.1	Bevölkerung sensibilisieren
Bemerkungen	Die Aktivitäten sind abzugleichen mit den analogen Massnahmen des Bundes, den ausbildungsbezogenen Massnahmen des Sicherheitsverbundes Schweiz und evtl. den Massnahmen der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren. Synergien mit der Kapo, insbesondere im präventiven Bereich nutzen (SKP). Mit den anderen Beteiligten ist zu klären, welche Unterstützung der Kanton Zürich beisteuern kann und welche Synergien genutzt werden können. Es ist auch eine Zusammenarbeit mit Verbraucherzentralen, Volkshochschulen oder der oder dem Datenschutzbeauftragten vorstellbar. Um den Fachkräftemangel zu lindern, kann er gegebenenfalls ein Angebot von berufsbegleitenden Studienplätzen oder Doktoratsstellen an ETH/UZH für die Nachwuchsförderung bereitstellen. Das soll neben technischen Aspekten auch die Disziplinen Psychologie, Organisationswissenschaften, Recht abdecken.

3.8 Handlungsfeld 8: Vernetzung und Austausch pflegen

A 8.1	Vernetzung und Austausch pflegen
Beschreibung	Neben den bereits in anderen Handlungsfeldern aufgeführten Aktivitäten zur Vernetzung betreibt der Kanton Zürich auch einen Erfahrungsaustausch mit den Nachbarländern sowie mit nationalen und internationalen Gremien und Expertinnen und Experten im Cyberbereich.[4]
Ergebnisse, Dienstleistungen	– Organisationen und Ansprechpersonen bezeichnet – Periodischer Austausch geplant, durchgeführt
Zielgruppe(n)	– Kantonale Verwaltung – Weitere Organe des Kantons – Bund – Internationale Organisationen – Forschung
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung	Kantonales Zentrum für Cybersicherheit
Meilensteine	Bis Q2/23 Aufbau Ab Q3/23 Umsetzung, Begleitung
Aufwand Initialisierung	Für diese Aufgabe entstehen weder Sachkosten noch Kosten für externe Dienstleistungen.
Aufwand laufender Betrieb	Offen; abhängig von Massnahmen aus dem Konzept
Bemerkungen	Die Aufgabe ist in Abhängigkeit der Aufgaben 3.1 sowie 3.3 bis 3.7 zu planen, um Doppelspurigkeiten zu vermeiden.

[4] Dazu gehören u.a. das NCSC des Bundes, Kantone, Baden-Württemberg (Ministerium des Inneren, für Digitalisierung und Kommunen / Cybersicherheitsagentur Baden-Württemberg), die Agentur der Europäischen Union für Cybersicherheit (ENISA), die Stiftung SWITCH sowie weitere Organisationen und Unternehmen, die sich mit Informationssicherheit und dem Schutz vor Cyberrisiken auseinandersetzen (Liste nicht abschliessend).

3.9 Handlungsfeld 9: Auf neue Situationen reagieren

A 9.1	Auf neue Situationen reagieren (Reserve)
Beschreibung	Um auf neue Bedrohungslagen oder neue Entwicklungen schnell und effizient reagieren zu können, steht eine monetäre Reserve zur Verfügung Die Freigabe der Mittel benötigt einen Entscheid der Kerngruppe Cyber.
Ergebnisse, Dienstleistungen	Finanzielle Ressourcen, um auf neue Gefahren effizient mit entsprechenden Massnahmen reagieren zu können
Zielgruppe(n)	– Kantonale Verwaltung – Weitere Organe des Kantons – Bund – Internationale Organisationen – Forschung
Zuständigkeit	Cyber-Koordinator/in
Mitwirkung	Kantonales Zentrum für Cybersicherheit
Meilensteine	Reserve
Aufwand Initialisierung	Bis Q2/22 Aufbau Ab Q3/22 Umsetzung, Begleitung
Aufwand laufender Betrieb	Rund Fr. 200 000/Jahr
Bemerkungen	Die Erfahrungen des Bundes zeigen, dass ein gewisser Spielraum für unvorhergesehene Massnahmen im Bereich des Cyberschutzes wichtig ist.

4. Aufbau der Organisation

Der Kanton Zürich schafft eine übergeordnete Organisation[5] des Kantons im Bereich Cybersicherheit. Die Verantwortlichkeiten für die Aufgaben sowie die organisatorische Einbettung der Rollen orientiert sich an der übergeordneten Organisation des Bundes[6].

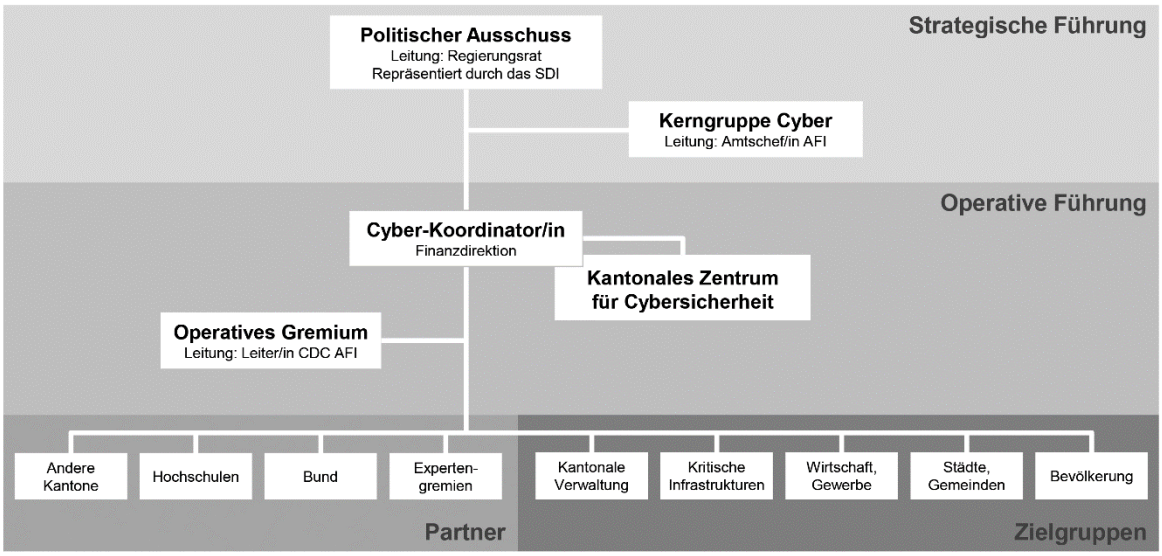


Abbildung 3: Organigramm der kantonalen Cyberorganisation

4.1 Politischer Ausschuss

Im Kanton Zürich nimmt der Regierungsrat die übergeordnete politische Verantwortung für die Cybersicherheit wahr. Die strategische Führung wird dem Gremium SDI übertragen.

4.2 Kerngruppe Cyber

Die Kerngruppe Cyber ist ein beratendes Gremium und unterstützt das SDI bei strategischen Entscheiden im Bereich Cybersicherheit. Die Kerngruppe stärkt die Zusammenarbeit innerhalb der kantonalen Verwaltung zwischen den drei Bereichen Cybersicherheit, Strafverfolgung und Cyber Defence sowie mit den Zielgruppen ausserhalb der kantonalen Verwaltung.

---

[5] Die Organisation innerhalb der kantonalen Verwaltung ist beschrieben im Geschäftsorganisationskonzept «IKT-Sicherheit» vom 29. Juni 2020. Dieses ist nach Freigabe der übergeordneten Cyberorganisation entsprechend anzupassen auf die neuen Gegebenheiten.

[6] https://www.newsd.admin.ch/newsd/message/attachments/56943.pdf

Die Kerngruppe Cyber setzt sich wie folgt zusammen:

- Leitung: Amtschefin oder Amtschef des Amtes für Informatik
- Cyber-Koordinatorin oder Cyber-Koordinator
- Staatsanwaltschaft
- Kantonspolizei
- Kantonale Führungsorganisation
- Kommunikationsverantwortliche oder Kommunikationsverantwortlicher des kantonalen Zentrums für Cybersicherheit
- Vertreterin oder Vertreter einer kantonalen kritischen Infrastruktur

Die Kerngruppe Cyber nimmt folgende Aufgaben wahr:

- sorgt für die Erarbeitung der gesetzlichen und anderer Rahmenbedingungen und beantragt diese bei der SDI bzw. dem Regierungsrat zur Umsetzung,
- berät das SDI zu Anträgen aus der Fachgruppe Informationssicherheit,
- definiert im Auftrag des SDI das Dienstleistungsangebot im Bereich Cybersicherheit,
- überprüft die operative Umsetzung anhand der definierten bzw. erreichten Ziele der Cybersicherheitsstrategie,
- genehmigt den von der Fachgruppe Informationssicherheit vorgelegten jährlichen Auditplan,
- beurteilt die Bewältigung von Cybervorfällen,
- zieht Lehren aus den Cybervorfällen der eigenen Organisation oder der Umwelt,
- unterstützt bei Differenzen in der kantonalen Cyberorganisation.

Das Gesamtprogramm und die Umsetzung der Cybersicherheitsstrategie sowie der Betrieb werden regelmässig durch eine externe Qualitätsmanagerin oder einen externen Qualitätsmanager überprüft. Auftraggeberin für diese Überprüfung ist die Kerngruppe Cyber.

4.3 Cyber-Koordinator/in

Die Cyber-Koordinatorin oder der Cyber-Koordinator nimmt innerhalb des Kantons, aber auch im Verhältnis zu den Behörden auf Bundesebene die Rolle der zentralen Anlaufstelle ein und stellt die Vernetzung zwischen den staatlichen und privaten Akteuren sicher. Sie oder er steht dem kantonalen Zentrum für Cybersicherheit vor und wird von diesem bei ihren oder seinen Aufgaben unterstützt. Die Cyber-Koordinatorin oder der Cyber-Koordinator rapportiert direkt an den Finanzdirektor. Ihre oder seine Rolle wird von der oder dem Informationssicherheitsbeauftragten des Kantons wahrgenommen. Schliesslich repräsentiert die Cyber-Koordinatorin oder der Cyber-Koordinator den Kanton Zürich in Cyberbelangen.

Die Cyber-Koordinatorin oder der Cyber-Koordinator nimmt folgende Aufgaben wahr:

- verfolgt die Cyberentwicklung,
- stellt den Austausch mit der strategischen Führung, der politischen Ebene und der Kantonspolizei sicher,
- beurteilt das Sicherheitsdispositiv,
- unterstützt im Krisenfall,
- führt das integrierte Risikomanagement Informationssicherheit und Krisenmanagement Cybersicherheit; pflegt den zugehörigen «Werkzeugkasten»,
- pflegt den Austausch mit dem Delegierten des Bundes für Cybersicherheit, mit dem Nationalen Zentrum für Cybersicherheit, mit der Schweizerischen Informatikkonferenz und mit dem Sicherheitsverbund Schweiz,
- repräsentiert den Austausch mit gleichgestellten Funktionen in anderen Kantonen,
- repräsentiert den Kanton Zürich in Cyberbelangen,
- erstellt Ausbildungsunterlagen und führt Schulungen für die Sensibilisierung von Verwaltung, Unternehmen und Bevölkerung zur Stärkung der Risiko- und Sicherheitskultur durch,
- koordiniert die Massnahmenumsetzung der Nationalen Strategie zum Schutz vor Cyber-Risiken im Kanton Zürich,
- pflegt den Kontakt mit der Wirtschaft, insbesondere mit den kantonalen kritischen Infrastrukturen sowie mit den Hochschulen und den relevanten Forschungsgruppen,
- koordiniert Übungen im Krisenstab mit den kantonalen kritischen Infrastrukturen,
- hält das Regelwerk Informationssicherheit aktuell, verbreitet es und stösst bei Bedarf Schulungen an,
- ordnet Audits an.

Situativ nimmt die Cyber-Koordinatorin oder der Cyber-Koordinator zusätzlich folgende Aufgaben wahr:

- erstellt Anträge an die politische Ebene:
  - Gesetzliche Vorgaben (Cybergesetz oder Cyberverordnung)
  - Budget für die Umsetzung der Massnahmen zur Erhöhung der Cybersicherheit
  - Umsetzung von Massnahmen
- beaufsichtigt Cybervorfälle, definiert Sofortmassnahmen und zieht Lehren aus dem Vorfall,
- unterstützt die Strafverfolgungsbehörden.

4.4 Kantonales Zentrum für Cybersicherheit

Das kantonale Zentrum für Cybersicherheit fördert die kantonale Risiko- und Sicherheitskultur, es stärkt die operative Informationssicherheit, es pflegt die Vernetzung und den Austausch und es führt die Geschäftsstelle einschliesslich Programmleitung, Projektmanagement-Office und Koordination.

Das kantonale Zentrum für Cybersicherheit unterstützt die Cyber-Koordinatorin oder den Cyber-Koordinator und nimmt folgende Aufgaben wahr:

- Kantonale Risiko- und Sicherheitskultur fördern
- Operative Informationssicherheit stärken
- Vernetzung und Austausch pflegen
- Geschäftsstelle führen einschliesslich Programmleitung, Projektmanagement-Office und Koordination

Das kantonale Zentrum für Cybersicherheit baut entsprechend den Empfehlungen des Sicherheitsverbundes Schweiz auf den bereits bestehenden Strukturen innerhalb der kantonalen Verwaltung auf. Es stellt den Direktionen und der Staatskanzlei eine Reihe Dienstleistungen im Bereich Cybersicherheit zur Verfügung, die sie nutzen können. Damit werden die Direktionen und die Staatskanzlei bei Cybersicherheitsaufgaben unterstützt und können sich auf ihre Kernaufgaben konzentrieren; gleichzeitig wird die Wahrung der Sorgfaltspflicht in der Informationssicherheit gewährleistet. Die Zusammenarbeit innerhalb der kantonalen Verwaltung ist im Geschäftsorganisationskonzept Informationssicherheit festgelegt.

Dem kantonalen Zentrum für Cybersicherheit steht neben den eigenen Mitarbeitenden ein externer Expertenpool mit Spezialisten der Informationssicherheit[7] zur Verfügung.

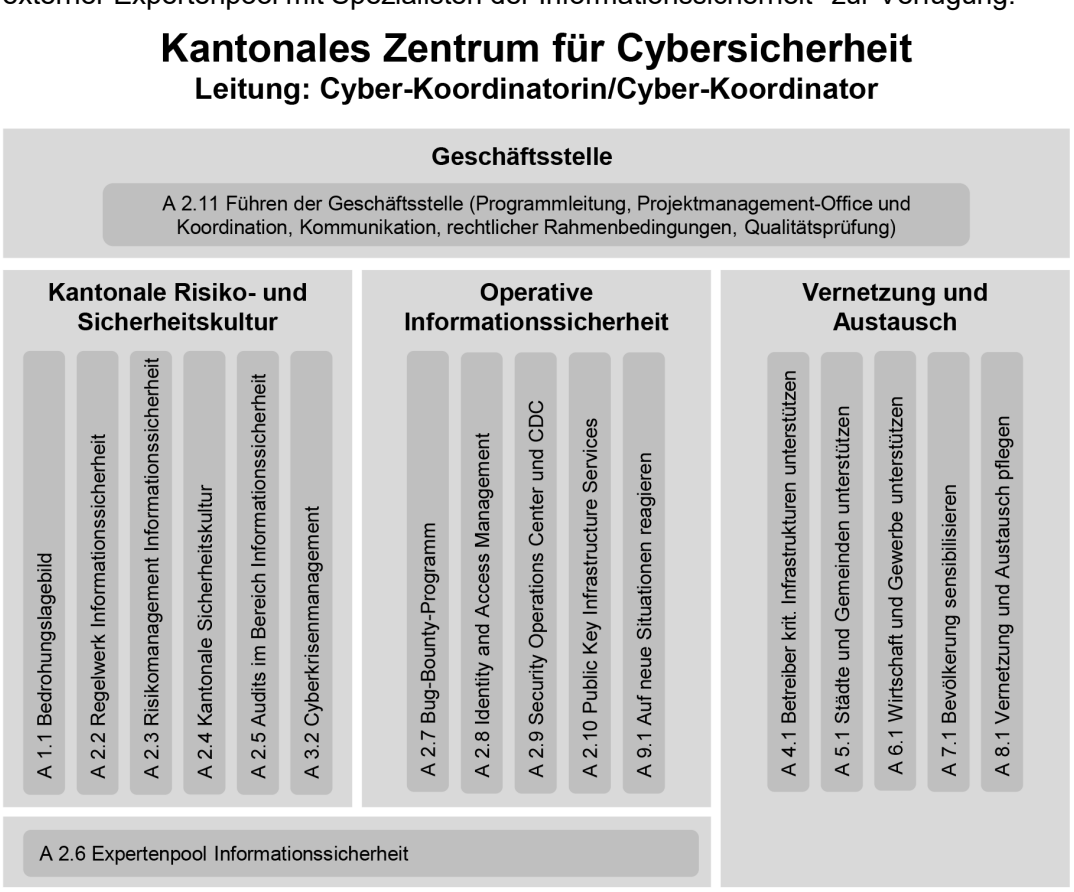


Abbildung 4: Gliederung und Aufgaben des kantonalen Zentrums für Cybersicherheit

[7] Vgl. RRB Nrn. 1193/2020 (Informationssicherheit, Umsetzung in den Direktionen und der Staatskanzlei, Stellenpläne, gebundene Ausgabe) und 811/2021 (Rahmenverträge für Expertenpool Informationssicherheit, Vergabe)

Das kantonale Zentrum für Cybersicherheit ist organisatorisch in die Finanzdirektion eingegliedert. Der Umgang mit Cyberrisken bedingt einen engen Austausch mit den Fachexpertinnen und -experten im Amt für Informatik, erfordert ein Abwägen zwischen geeigneten Massnahmen und kann finanzielle und personelle Konsequenzen nach sich ziehen; aus diesen Gründen ist die Nähe zur Finanzdirektion zweckmässig. Diese Eingliederung folgt auch dem Ansatz des Bundes, wo das nationale Zentrum für Cybersicherheit dem Eidgenössischen Finanzdepartement unterstellt ist.

4.5 Operatives Gremium

Das operative Gremium ist wie folgt zusammengesetzt:

- Leitung: Leiterin oder Leiter Cyber Defence Center des Amtes für Informatik
- Kantonale Führungsorganisation
- Informatik (Informationssicherheit und Kommunikation)
- bei Bedarf: Staatsanwaltschaft und Kantonspolizei

Die Kantonale Führungsorganisation ist dann in die Bewältigung von Krisenfällen einbezogen und übernimmt die Führung, wenn der Krisenfall von Belang für den Bevölkerungsschutz ist. Bei den weiteren Aufgaben nimmt sie keine aktive Rolle ein; sie stellt jedoch sicher, dass der Wissensaustausch mit den anderen Mitgliedern zuverlässig funktioniert.

Wenn Cybervorfälle strafrechtlich relevant sind, werden sie grundsätzlich gleich behandelt wie andere Ereignisse, bei denen Staatsanwaltschaft, Kantonspolizei und weitere Einheiten involviert sind. Die betroffene Stelle, ein Cyber Defence Center oder das Amt für Informatik, stellt den Vorfall fest und erstattet gegebenenfalls Anzeige, die Kantonspolizei ist zuständig für die Beweissicherung, und die Staatsanwaltschaft fällt die entsprechenden Entscheide in Bezug auf eine potenzielle Strafverfolgung.

Das operative Gremium:

- verfolgt die Cyberbedrohungslage
  - intern: Incident Management, Monitoring
  - extern: Meldungen des NCSC, Informationen aus frei verfügbaren offenen Quellen
- beurteilt die Cyberentwicklung in ihren Bereichen sowie Massnahmen zum Schutz vor Cyberrisiken,
- bewältigt Cybervorfälle und unterstützt in einem schweren Cyberereignis (ausserordentliche Lage) als Stabsorganisation den Regierungsrat,
- stellt sicher, dass seine Organisation über die notwendigen Ressourcen verfügt (qualifizierte Mitarbeitende, Hard- und Software).

4.6 Zielgruppen und Partner

Der Kanton Zürich sucht die Zusammenarbeit im Bereich Cybersicherheit. Er pflegt den Austausch mit dem Bund, anderen Kantonen, Städten und Gemeinden, Organisationen und Unternehmen, national und international, um die Vernetzung zu verstärken. Insbesondere unterstützt der Kanton Zürich das eigenverantwortliche Handeln der Zielgruppen. Er informiert und sensibilisiert, er fördert und vernetzt, und er kann bei Bedarf gezielt unterstützen.

Sein klarer Schwerpunkt liegt auf der Unterstützung der kantonalen Verwaltung und den kantonsnahen Organisationen im Kanton Zürich. Hier wird er einen Grossteil seiner vorgesehenen Ressourcen einsetzen.

Daneben pflegt er eine Zusammenarbeit mit:
- Betreibern kritischer Infrastrukturen des Kantons Zürich
- Städten und Gemeinden
- Wirtschaft und Gewerbe des Kantons Zürich
- Zürcher Wohn- und Arbeitsbevölkerung

Zudem pflegt der Kanton Zürich den Erfahrungsaustausch mit:
- Hochschulen (insbesondere ETH und UZH)
- anderen Kantonen und dem Bund
- nationalen und internationalen Fachgremien und Behörden

4.7 Zusammenspiel mit dem Geschäftsorganisationskonzept Informationssicherheit

Die Cybersicherheitsstrategie erlaubt die Vernetzung aller relevanten Cyberakteure innerhalb der Verwaltung (Sicherheit, Verfolgung und Verteidigung), sie ermöglicht den Einbezug aller externen Zielgruppen (kritische Infrastrukturen usw.), und sie schafft die Basis für eine zentrale Bereitstellung von Dienstleistungen im Bereich Cybersicherheit durch das kantonale Zentrum für Cybersicherheit zugunsten der Direktionen und der Staatskanzlei. Damit werden die Direktionen und die Staatskanzlei bei Cybersicherheitsaufgaben unterstützt und können sich auf ihre Kernaufgaben konzentrieren. Gleichzeitig wird die Wahrung der Sorgfaltspflicht in der Informationssicherheit gewährleistet.

Die Zusammenarbeit innerhalb der kantonalen Verwaltung ist im Geschäftsorganisationskonzept Informationssicherheit festgelegt. Hier werden die bestehenden Strukturen und Prozesse genutzt. Das Geschäftsorganisationskonzept Informationssicherheit (Version 1.0, RRB Nr. 1193/2020) beschreibt die Ablauforganisation der Informationssicherheit in der kantonalen Verwaltung. Diese Organisation sowie die definierten Prozesse und Rollen bleiben bestehen. Sie werden erweitert mit den zusätzlichen Gremien und Strukturen.

Mit der Cybersicherheitsstrategie werden dadurch bestehende Strukturen entlastet, und Cybersicherheitsdienstleistungen können zentral in hoher Qualität für alle Direktionen und die Staatskanzlei bereitgestellt werden.

4.8 Zusammenarbeit mit der Kantonalen Führungsorganisation

Das kantonale Zentrum für Cybersicherheit stellt sicher, dass die Umsetzung der Cybersicherheitsstrategie den Ansprüchen des integralen Risikomanagements und dem Risikomanagement Bevölkerungsschutz genügt. Es deckt als Fachstelle das Management des Teils «Cyberrisiken» ab und sorgt dafür, dass das benötigte Expertenwissen eingebracht wird und keine inhaltlichen oder methodischen Widersprüche entstehen. Die Zusammenarbeit ist über die Mitwirkung im Fachstab der Kantonalen Führungsorganisation geregelt (§ 3 Abs. 3 Verordnung über die strategische Führung und den Einsatz der kantonalen Führungsorganisation vom 22. Dezember 2010).

Bei der Führung im Ereignisfall (ausserordentliche Lage und andere Lagen) und der Bewältigung gelten unverändert die gesetzlichen Zuständigkeiten. Die Schnittstellen und Unterstützungsangebote insbesondere zwischen dem Amt für Informatik und der Kantonalen Führungsorganisation sind bekannt. Die Führungsorganisation in der Verwaltungseinheit bleibt auch im Ereignis unverändert.

5. Umsetzungsschritte

Der Schwerpunkt liegt in der ersten Phase bis Ende 2023 auf den Handlungsfeldern 1, 2 und 3, wo es um die Bedrohungslage, die Stärkung der kantonalen Verwaltung und den Umgang mit Vorfällen geht.

In einer zweiten Phase ab 2024 richten sich die Anstrengungen zusätzlich auf die weiteren Zielgruppen des Kantons, insbesondere auf seine kritischen Infrastrukturen.

Im Hinblick auf diese Phase muss auch die Organisationsstruktur im Bereich Cybersicherheit überprüft werden.

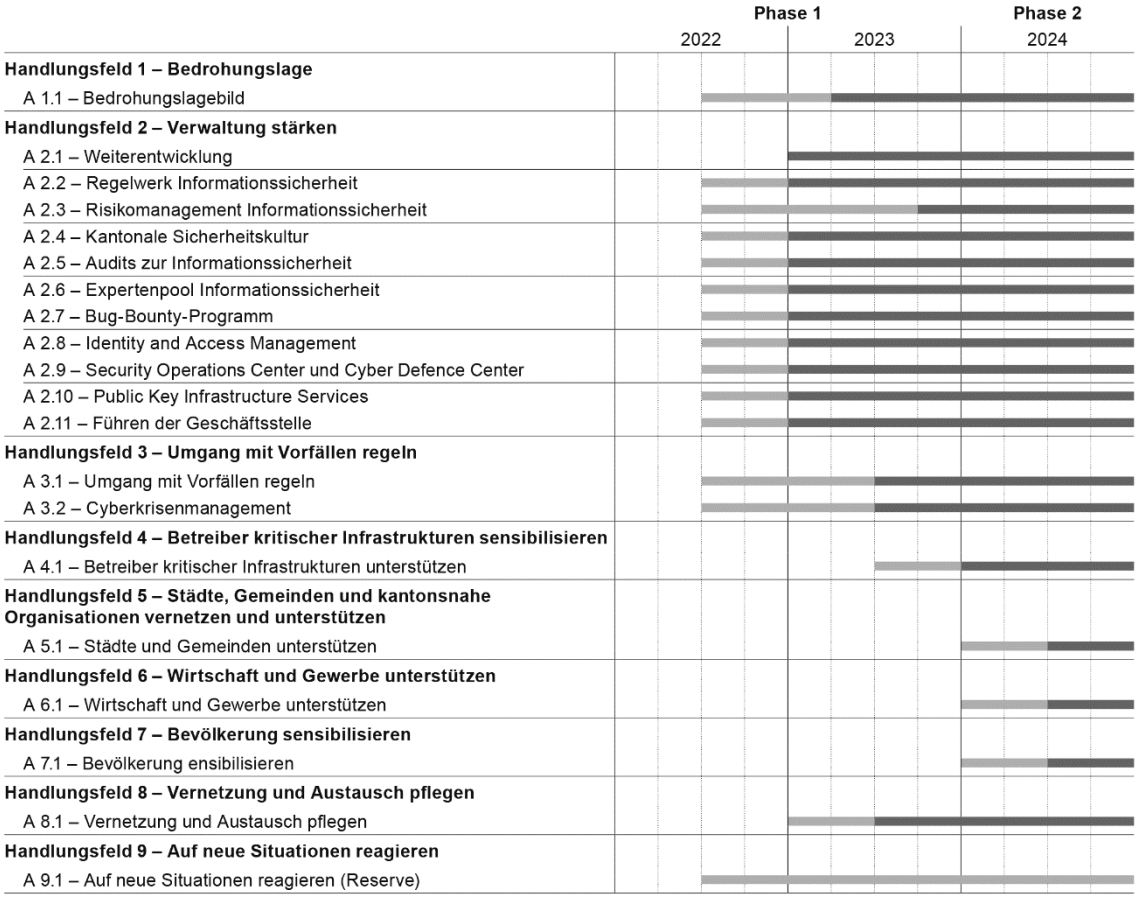


Abbildung 5: Zeitplan zur Umsetzung der Strategie mit Schwerpunkt der Zielgruppen

6. Ressourcen

6.1 Personal

Es werden 18 unbefristete Vollzeitstellen geschaffen. Die Stellen werden den Direktionen wie folgt zugeordnet:

Anzahl Stellen	Auf-gabe	Richtpositionsumschreibung/Rolle	Leistungs-gruppe	Klasse VVO
Sicherheitsdirektion				
1.0	A 2.9	Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «SOC / CDC / Security Incident Analyst»)	3100	21
Finanzdirektion				
1.0	A 2.3	Informatikspezialist/in mbA (Leiter/Leiterin Informa-tionssicherheits- Experte/-Expertin «Risikomanage-ment»)	4620	23
3.0	A 2.3	Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «Risikomanagement»)	4620	22
1.0	A 2.4	Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «Security-Awareness»)	4620	22
1.0	A 2.5	Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «Audit»)	4620	22
1.0	A 2.6	Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin Verstärkung Expertenpool Informa-tionssicherheit)	4620	22
2.0	A 2.8	Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «IAM»)	4610	21
3.0	A 2.9	Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «SOC / CDC / Security Incident Analyst»)	4610	21
2.0	A 2.10	Informatikspezialist/in mbA (Informationssicherheits-Experte/-Expertin «PKI»)	4610	21
1.0	A 2.11	Informatikspezialist/in mbA (Programm-Manager/in)	4620	20
1.0	A 2.11	Informatikspezialist/in mbA (Experte/Expertin Pro-jektmanagement-Office, Koordination)	4620	13
1.0	A 2.11	Adjunkt/in (Experte/Expertin Kommunikation)	4620	20
18.0 unbefristete Vollzeitstellen				

Tabelle 1: Übersicht über die zu schaffenden Stellen

Die Stellenbesetzung soll parallel zu den vorgesehenen Umsetzungsschritten erfolgen. Angestrebt wird eine Staffelung mit der Besetzung von sechs Stellen ab 1. Juli 2022, sechs Stellen ab 1. Januar 2023 und sechs Stellen ab 1. Januar 2024.

Für die Unterstützung bei der Stellenbesetzung soll ein externer Personaldienstleister beigezogen werden. Dafür wird mit Kosten von Fr. 250 000 zulasten der Erfolgsrechnung der Leistungsgruppe Nr. 4620, IKT-Sicherheitsbeauftragter, gerechnet.

Die Personalkosten lassen sich wie folgt zusammenfassen:

	ab 1. Juli 2022	2023	ab 2024
Personalkosten; davon:	530 000	2 080 000	3 050 000
LG Nr. 3100 Kantons-polizei		170 000	170 000
LG Nr. 4610, Amt für Informatik	85 000	680 000	1 190 000
LG Nr. 4620, Informatik-sicherheitsbeauftragter	445 000	1 230 000	1 690 000

Tabelle 2: Schätzung der anfallenden personellen Kosten (in Franken)

Die Überprüfung der Einreihung sämtlicher zu schaffenden Stellen erfolgte durch die perinnova compensation GmbH.

Der Vergleich mit der Anzahl Stellen, die sich heute in der Sicherheitsdirektion und der Finanzdirektion mit den Fragen der Cybersicherheit auseinandersetzen, ergibt folgendes Bild:

	Heutige Anzahl Stellen	Anzahl Stellen nach der Umsetzung der Cybersicherheitsstrategie
Sicherheitsdirektion (einschliesslich SOC KAPO)	**5**	**6**
Finanzdirektion	**8**	**25**
davon Stellen der Cyber-Koordinatorin oder dem Cyber-Koordinator (Leistungsgruppe Nr. 4620) unterstellt	1	11
davon Stellen der Leiterin oder dem Leiter Cyber Defence Center des AFI (Leistungsgruppe Nr. 4610) unterstellt	7	14
Fünf weitere Direktionen und Staatskanzlei	**6**	**6**
Total	**19**	**37**

Tabelle 3: Vergleich mit heutiger Stellenanzahl im Bereich Cybersicherheit

Benchmarking

Die Grösse der zukünftigen Cyberorganisation des Kantons Zürich ist vergleichbar mit der Grösse der Cyberorganisationen des Kantons Waadt sowie des Bundes.

Verwaltung/ Organisation	Anzahl Mitarbeitende mit Cybersicherheitsaufgaben in zentraler Sicherheitsorganisation	Anzahl Mitarbeitende mit Cybersicherheitsaufgaben dezentral in den Departementen, Direktionen und Ämtern	Grösse der Organisation (Anzahl Mitarbeitende)	Anzahl betreute Arbeitsplätze	Anzahl betreute Applikationen	Anzahl Einwohnerinnen und Einwohner
Kanton Zürich (Soll gemäss RRB)	24	13	30 000	20 000	1 500	1 550 000
Kanton Waadt (Stand Februar 2022)	30		15 000	15 000	3 000	800 000
Bund (Stand Februar 2022	40	25 Vollzeitstellen; 76 Teilzeitstellen	35 000	43 000	1 200	8 600 000

Tabelle 4: Vergleich Kenngrössen andere Kantone und Bund

6.2 Sachkosten und Kosten externer Dienstleistungen

Gewisse Leistungen werden von externen Dienstleisterinnen und Dienstleistern eingekauft und es entstehen Sachkosten. Die Tabelle 5 zeigt die entsprechenden Kosten für alle ausgewiesen neuen Aufgabenbereiche und Projekte, die im Zusammenhang mit der Cybersicherheitsstrategie stehen.

Externe Dienstleistungen (Honorare)

Aufgabenbereich	Projektkosten (einmalig, in Franken) 2022	2023	2024	Total (einmalig, in Franken)	Betriebskosten (wiederkehrend, in Franken)
A 1.1 Bedrohungslagebild kennen	50 000	50 000		100 000	
A 2.1 Überprüfung und Weiterentwicklung Cybersicherheitsstrategie einschliesslich Umsetzungsdokument		25 000	25 000	50 000	25 000
A 2.2 Regelwerk Informationssicherheit			100 000	100 000	100 000
A 2.3 Integriertes Risikomanagement Informationssicherheit	350 000	50 000	50 000	450 000	50 000
A 2.4 Kantonale Sicherheitskultur	75 000	150 000	150 000	375 000	150 000

Aufgabenbereich	Projekt-kosten (einmalig, in Franken) 2022	2023	2024	Total (einmalig, in Franken)	Betriebs-kosten (wieder-kehrend, in Franken)
A 2.5 Audits im Bereich Informationssicherheit	175 000	350 000	350 000	875 000	350 000
A 2.7 Bug-Bounty-Programm	125 000	250 000	250 000	625 000	250 000
A 2.8 Identity and Access Management		200 000	200 000	400 000	
A 2.9 Security Operations Center und Cyber Defence Center		200 000	200 000	400 000	
A 2.10 Public Key Infrastructure Services		125 000	75 000	200 000	
A 2.11 Führen der Geschäftsstelle	25 000	25 000	25 000	75 000	25 000
A 3.2 Cyberkrisenmanagement	50 000	100 000	100 000	250 000	100 000
A 4.1 Betreiber kritischer Infrastrukturen unterstützen		25 000			
A 5.1 Städte und Gemeinden unterstützen		25 000		25 000	
A 6.1 Wirtschaft und Gewerbe unterstützen		25 000		25 000	
A 7.1 Bevölkerung sensibilisieren		25 000		25 000	
A 9.1 Auf neue Situationen reagieren (Reserve)	100 000	200 000	200 000	500 000	200 000
Total	**950 000**	**1 825 000**	**1 725 000**	**4 500 000**	**1 250 000**

Tabelle 5: Schätzung der Kosten für externe Dienstleistungen (in Franken)

Sachkosten (Hardwarekomponenten, Softwarelizenzkosten und Informatiknutzungsaufwand)

Aufgabenbereich	Projektkosten (einmalig, in Franken) 2022	2023	2024	Total (einmalig, in Franken)	Betriebskosten (wiederkehrend, in Franken) ab 2025
A 1.1 Bedrohungslagebild		25 000	25 000	50 000	25 000
A 2.3 Integriertes Risikomanagement Informationssicherheit	125 000	250 000	250 000	625 000	250 000
A 2.4 Kantonale Sicherheitskultur	50 000	100 000	100 000	250 000	100 000
A 2.7 Bug-Bounty-Programm	75 000	75 000	75 000	225 000	75 000
A 2.8 Identity and Access Management		700 000	700 000	1 400 000	700 000
A 2.9 Security Operations Center und Cyber Defence Center		800 000	800 000	1 600 000	800 000
A 2.10 Public Key Infrastructure Services (PKI)		350 000	350 000	700 000	350 000
Total	**250 000**	**2 300 000**	**2 300 000**	**4 850 000**	**2 300 000**

Tabelle 6: Schätzung der anfallenden Sachkosten (in Franken)

Die Kosten für den externen Personaldienstleister, für externe Dienstleistungen und die Sachkosten lassen sich wie folgt zusammenfassen:

	Projektkosten (einmalig, in Franken) 2022	2023	2024	Total (einmalig, in Franken)	Betriebskosten (wiederkehrend, in Franken) ab 2025
Kosten für externen Personaldienstleister	125 000	125 000		250 000	
Kosten externe Dienstleistungen	950 000	1 825 000	1 725 000	4 500 000	1 250 000
Sachkosten	250 000	2 300 000	2 300 000	4 850 000	2 300 000
Total	**1 325 000**	**4 250 000**	**4 025 000**	**9 600 000**	**3 550 000**

Tabelle 7: Schätzung der anfallenden externen Dienstleistungen und Sachkosten (in Franken)

A. Anhang: Abkürzungen und Glossar

AFI	Amt für Informatik
AISR	Allgemeine Informationssicherheitsrichtlinie
AWA	Amt für Wirtschaft und Arbeit
BCM, Business Continuity Management	Business Continuity Management; betriebliches Kontinuitätsmanagement; Aufbau und Betrieb eines Notfall- und Krisenmanagements, damit Kernprozesse von Organisationen und Unternehmen bei schweren Ereignissen nicht oder nur kurzfristig unterbrochen werden.
BISR	Besondere Informationssicherheitsrichtlinien
BIT	Bundesamt für Informatik und Telekommunikation
Blue-Team	Das blaue Team übernimmt bei Cyberübungen die Rolle des Verteidigers und versucht dabei, das System, die Plattform, die Daten zu schützen.
Bug-Bounty-Programm	Programm zum Entdecken von Sicherheitslücken in Software, die mit den klassischen Testmethoden verborgen bleiben.
CASB	Cloud Access Security Broker; eine lokale oder Cloud-basierte Software, die sich zwischen der lokalen Infrastruktur einer Organisation und dem Netzwerk eines Cloud-Anbieters befindet. Sie überwacht die Aktivitäten und setzt Sicherheitsrichtlinien über die Grenzen der eigenen Infrastruktur hinaus durch.
CDC	Cyber Defence Center; Weiterentwicklung eines SOC
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
Cyberangriff	Beabsichtigte unerlaubte Handlung einer Person oder einer Gruppierung im Cyberraum, um die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen und Daten zu beeinträchtigen; dies kann je nach Art des Angriffs auch zu physischen Auswirkungen führen.
Cyberbedrohung	Vorgang, der zum Eintreten eines Cybervorfalls führen kann.
Cyberkriminalität	Cyberkriminalität im engeren Sinn betrifft Straftaten, die mithilfe der Informations- und Kommunikationstechnologien (IKT) verübt werden oder sich Schwachstellen dieser Technologien zunutze machen. Cyberkriminalität im weiteren Sinn nutzt das Internet als Kommunikationsmittel, wobei die sich bietenden Möglichkeiten wie z.B. der E-Mail-Verkehr oder der Austausch bzw. das Bereitstellen von Dateien für unlautere Zwecke missbraucht werden. Diese Aktivitäten sind nicht neu, aber die dabei verwendeten Tat- und Speichermedien (z.B. E-Mail, Instant-Messaging-Dienste, elektronische Datenträger) sind neu.
Cyberraum	Die Gesamtheit der durch das Internet weltweit erreichbaren Informationsinfrastrukturen
Cyberrisiken	Das Produkt der Eintrittswahrscheinlichkeit und des Schadenausmasses von Cybervorfällen
Cybersicherheit	Anzustrebender Zustand innerhalb des Cyberraums, bei dem die Kommunikation und der Datenaustausch zwischen Informations- und Kommunikationsinfrastrukturen wie ursprünglich beabsichtigt funktionieren. Dieser Zustand wird mit Massnahmen der Informationssicherheit und der Cyber Defence erreicht.
Cybervorfall	Beabsichtigtes oder unbeabsichtigtes Ereignis, das im Cyberraum zu einem Vorgang führt, der die Integrität, Vertraulichkeit oder Verfügbarkeit von Daten und Informationen beeinträchtigt und zu Fehlfunktionen führen kann.

Datenschutzbeauftragte/r, DSB	Die oder der Datenschutzbeauftragte beaufsichtigt als unabhängige Aufsichtsbehörde die Datenbearbeitungen der öffentlichen Organe im Kanton Zürich. Die Behörde berät öffentliche Organe und Privatpersonen zu Fragen des Datenschutzes und der Informationssicherheit, führt Kontrollen durch und informiert die Öffentlichkeit über die Anliegen des Datenschutzes und der Informationssicherheit.
EDR	Endpoint Detection and Response; Software, mit deren Hilfe potenziell böswillige Aktivitäten auf Clients und Servern im lokalen Netz entdeckt werden können.
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ENISA	European Union Agency for Cybersecurity
ETH	Eidgenössische Technische Hochschule Zürich
FAGIS	Fachgruppe IKT-Sicherheit
FD	Finanzdirektion
FIRST	Forum of Incident Response and Security Teams; weltweit agierender Dachverband von CERT und IT-Sicherheitsfachleuten
FTE	Full Time Equivalent, Vollzeitäquivalent, 100%-Stelle, Kennzahl in der Personalverwaltung
govCERT	Nationales Computer Emergency Response Team
Governance	Steuerung und Regelung in Organisation
IAM	Identity and Access Management; technische Lösungen zur Verwaltung digitaler Identitäten und deren Zugriffe auf verschiedene Anwendungen und Systeme; erlaubt, dass Personen und Abteilungen mit den entsprechenden Zugriffsrechten auf Unternehmensressourcen zugreifen können.
IKS	Internes Kontrollsystem
IDG	Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (LS 170.4)
IKT	Informations- und Kommunikationstechnologien
IVSV	Verordnung über die Informationsverwaltung und -sicherheit vom 3. September 2019 (LS 170.8)
Informationssicherheit / IKT-Sicherheit	Informationssicherheit (oder IKT-Sicherheit) ist die Unversehrtheit der Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit eines informations- und kommunikationstechnischen Systems und der darin verarbeiteten und gespeicherten Daten.
ISAC	Information Sharing und Analysis Center
ISID	IKT-Sicherheitsbeauftragte/r der Direktion oder Staatskanzlei
ISIK	IKT-Sicherheitsbeauftragte/r des Kantons Zürich
ISMS	Informationssicherheits-Managementsystem
Kanton Zürich	Die Regierung und Verwaltung des Kantons Zürich. Dabei mitgemeint sind auch all seine schützenswerten Güter (IT-Inventar).
Kapo	Kantonspolizei
KFO	Kantonale Führungsorganisation
KI	Kritische Infrastrukturen (auch: künstliche Intelligenz)
Krise, Krisenfall	Ein Ereignisfall, bei dem der ganze Kanton betroffen ist und die KFO involviert wird, weil es für den Bevölkerungsschutz relevant wird.
KRITIS	Kritische Infrastrukturen

Kritische Infrastrukturen	Prozesse, Systeme und Einrichtungen, die essenziell für das Wohlergehen der Bevölkerung bzw. das Funktionieren der Wirtschaft sind.
MSSP	Managed Security Service Provider; ein MSSP ist ein IT-Service-Anbieter, der sich auf Cybersicherheit spezialisiert hat und Systeme verwaltet und überwacht. Er sorgt für alle Updates und Upgrades und für Massnahmen im Ereignisfall.
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NCSC	Nationales Zentrum für Cybersicherheit
NDR	Network Detection and Response; laufende Analyse des Rohdatenverkehrs und/oder Datenflussaufzeichnungen in Netzwerken, um verdächtigen Datenverkehr in Netzwerken zu erkennen.
NIST	National Institute of Standards and Frameworks
PAM	Privileged Access Management; Systeme zur sicheren Verwaltung von Benutzerkonten, die über erhöhte Berechtigungen für kritische Unternehmensressourcen verfügen.
Penetration Testing	Prüfung der Sicherheit von Systemen und Anwendungen mit Mitteln und Methoden, die ein Angreifer anwenden würde, um unautorisiert in ein System einzudringen.
PT	Personentage
Ransomware	Erpressungssoftware, die den Zugriff auf Daten oder auf Systeme verhindert. Für die Entschlüsselung von Daten oder die Freigabe wird in der Regel ein Lösegeld gefordert.
RBAC	Role Based Access Control; Vergaben von Zugriffsrechten anhand definierter Rollen (z.B. Abteilung, Funktion, Standort), nicht an Einzelbenutzer eines Mitarbeitenden.
Red-Team	Das rote Team übernimmt bei Cyberübungen die Rolle des Angreifers und versucht, die Schutzmassnahmen zu überwinden.
Resilienz	Die Fähigkeit eines Systems, einer Organisation oder einer Gesellschaft, Störungen zu widerstehen und die Funktionsfähigkeit möglichst zu erhalten bzw. rasch wieder zu erlangen.
RR	Regierungsrat
RRB	Regierungsratsbeschluss
SDI	Gremium Steuerung Digitale Verwaltung und IKT
SECO	Staatssekretariat für Wirtschaft
SIK	Schweizerische Informatikkonferenz
SK	Staatskanzlei
SKI	Schutz kritischer Infrastrukturen
SKP	Schweizerische Kriminalprävention
SOC	Security Operations Center
SPOC	Single Point of Contact
SSO	Single-Sign-On
SVS	Sicherheitsverbund Schweiz
UZH	Universität Zürich
VDP, Vulnerability-Disclosure Policy	Vulnerability-Disclosure Policy; Regelung der Zusammenarbeit zwischen Unternehmen und Organisationen mit Hackern, um Schwachstellen zu erkennen.
WL	Wirtschaftliche Landesversorgung