

IT- Referat

Hauptabteilung I - IT-Strategie
und IT-Steuerung/IT-Controlling

Abteilung 4 - Informationssicher-
heitsmanagement

Leistungsschnitt 2.0 im Bereich Informationssicherheitsmanagement

Umsetzungskonzept

Version	1.0
Stand	Final
Datum	06.09.2021
Autor	RIT-I A4
Kontakt	ism@muenchen.de

Inhalt

1.	Management Summary	2
2.	Hintergrund	3
3.	Personalrechtliche und Verantwortungsperspektive	3
3.1.	Aktuelle Situation.....	3
3.2.	Organisatorisches Zielbild	5
3.3.	Umsetzungsmaßnahmen und Synergiepotentiale	6
4.	Fachliche Perspektive	8
4.1.	Konzeptueller Ansatz	8
4.2.	Fachliches Zielbild.....	9
4.3.	Umsetzungsmaßnahmen	10
5.	Pilotierung des Umsetzungskonzepts im MOR.....	11

1. Management Summary

Das vorliegende Dokument beschreibt ein Konzept zur Umsetzung der Inhalte des Leistungsschnitts 2.0 im Bereich des Informationssicherheitsmanagements der LHM (ISM) gemäß der Beschlussfassung des Stadtrats vom 28.7.2021 zur BV A01732.

Die Zielsetzung des Konzepts besteht darin, durch die zentrale Verankerung der Aufgaben des dezentralen Informationssicherheitsmanagements im IT-Referat (bisher in den Ref / Ebs verortet), die Effektivität in der Steuerung der Informationssicherheit der LHM stadtweit zu steigern sowie durch Standardisierungen in den Ref / Ebs Effizienzsteigerungen in der Aufgabendurchführung des dezentralen Informationssicherheitsmanagements zu erzielen.

Das Konzept beschreibt ein organisatorisches und ein fachliches Zielbild der Zentralisierung sowie Konzeptbausteine in Form konkreter Maßnahmen zur Erreichung der jeweiligen Zielsetzungen. Zusammengefasst ergeben sich folgende Maßnahmen, die zur Umsetzung des Leistungsschnitts 2.0 im Bereich des Informationssicherheitsmanagements der LHM notwendig sind.

Maßnahmenbündel „Personalrechtliche und Verantwortungsperspektive“

- Übergang der Dienstaufsicht der Mitarbeitenden im dezentralen Informationssicherheitsmanagement von den Referaten und Eigenbetrieben in das IT-Referat (RIT-I A4)
- Anpassungen im Aufgabegliederungsplan im Hinblick auf die Verortung der Aufgabe „dezentrales Informationssicherheitsmanagement“
- Regulatorische Anpassungen im Regelwerk IT-Sicherheit, um Themen wie Verantwortungsbereiche oder Befugnisse für die Rolle des / der dezentralen Informationssicherheitsbeauftragten im IT-Referat formal abzubilden.
- Organisationsanpassungen bei RIT-I A4 (aufbau- wie ablauforientiert)

Maßnahmenbündel „Fachliche Perspektive“

- Inhaltliche Entwicklung der stadtweiten Standards im dezentralen Informationssicherheitsmanagement auf Grundlage des fachlichen Zielbilds
- Kontinuierliche Fortschreibung und Verankerung der Standards in den entsprechenden Vorgehensweisen bzw. Prozessen des ISM der LHM
- Ausbildung konkreter fachlicher Tätigkeitsprofile für dezentrale Informationssicherheitsbeauftragte und entsprechende Kompetenzentwicklung
- Entwicklung fachlicher spezialisierter Teams für dedizierte Themenbereiche im dezentralen Informationssicherheitsmanagement, die einheitenübergreifend agieren

Vor diesem Hintergrund stellt Kapitel 2 die Rahmenbedingungen und Zielsetzungen des Umsetzungskonzepts vor, bevor in Kapitel 3 die personalrechtliche und Verantwortungsperspektive mit organisatorischem Zielbild und Maßnahmendarstellung beleuchtet wird. Kapitel 4 erläutert aufbauend die fachliche Perspektive des Umsetzungskonzepts in Verbindung mit der Darstellung des fachlichen Zielbilds sowie den zugehörigen Maßnahmen. In Kapitel 5 werden abschließend Aussagen zur geforderten Pilotierung des Umsetzungskonzepts im Mobilitätsreferat getroffen.

2. Hintergrund

Bei der Umsetzung des Leistungsschnitts 2.0 geht es gemäß Beschlussfassung darum, dass „die – bisher verteilt - in den Referaten und Eigenbetrieben angesiedelten IT-Aufgaben mit einem ähnlichen Aufgabenspektrum zentral an einer Stelle zu zusammengeführt“ (Beschlussfassung VV, 28.07.2021) werden.

Im Kontext der Informationssicherheit bedeutet dies, die Aufgabe „dezentrales Informationssicherheitsmanagement“ (dezISM) im RIT zu zentralisieren und festzulegen, auf welche Art und Weise dies erfolgen soll. Hierfür ist die Betrachtung dreier Perspektiven wesentlich.

Zum einen die **personalrechtliche Perspektive**, bei der es zu entscheiden gilt, in welchen Organisationseinheiten die Dienstaufsicht sowie die Fachaufsicht für die Mitarbeitenden liegen soll, die die Aufgabe dezISM durchführen.

Zum anderen die **Verantwortungsperspektive**, die sich darauf bezieht, in welcher Organisationseinheit die Durchführungs- und Ergebnisverantwortung („responsible / accountable“, gem. RACI-Modell, GPM LHM) sowie die Gesamtverantwortung (aus Sicht der Organisation LHM) für die Aufgabe dezISM liegt.

Und schließlich geht es um die **fachliche Perspektive**, die sich mit konkreten Aufgaben und entsprechenden Synergie- bzw. Effizienzpotentialen im Kontext des dezentralen Informationssicherheitsmanagements befasst.

Die Festlegung der konkreten Ausprägungen in allen drei Perspektiven erzeugt im Ergebnis das **Umsetzungskonzept**, das die Aspekte des Leistungsschnitts 2.0 im Bereich der Informationssicherheit der LHM abbildet.

In den folgenden Kapiteln werden die drei Perspektiven aus inhaltlicher Sicht beschrieben sowie das jeweilige Zielbild und zugehörige Umsetzungsmaßnahmen dargestellt.

3. Personalrechtliche und Verantwortungsperspektive

Die Aufgabe des dezentralen Informationssicherheitsmanagements ist einer von vier zentralen Verantwortungsbereichen im Informationssicherheitsmanagement der LHM. Zur besseren Einordnung des personalrechtlichen und verantwortungsbezogenen Blickwinkels wird im Folgenden zunächst die bestehende Situation skizziert (Kapitel 3.1), bevor das Zielbild des Umsetzungskonzepts (Kapitel 3.2) sowie entsprechende Maßnahmen (Kapitel 3.3) dargestellt werden.

3.1. Aktuelle Situation

Die vier Verantwortungsbereiche (oder auch Aufgabenfelder) im Informationssicherheitsmanagement sind wie folgt ausgestaltet bzw. in der Organisation verankert.

Stadtweites Informationssicherheitsmanagement

- ISM aus gesamtheitlicher Sicht der Verwaltung: Planung, Steuerung und Kontrolle der Informationssicherheit der LHM über alle Organisationseinheiten hinweg.
- Delegation der „Verantwortung für die laufenden Angelegenheiten des Informationssicherheitsmanagements“ durch den Oberbürgermeister an Dr. Rothenhöfer und Dr. Reeg.
- Bestellung von Dr. Reeg zum Informationssicherheitsbeauftragten der LHM.

Informationssicherheitsmanagement bei it@M

- ISM aus IT-Sicht: Planung, Steuerung und Kontrolle der Informationssicherheit bei it@M.
- Delegation der „Verantwortung für die IT-Sicherheit im RIT und bei it@M“ durch RIT-L / it@M - WL an Dr. Reeg.
- Bestellung von Herrn Adamczyk (RIT-I A4) zum Informationssicherheitsbeauftragten von it@M.
- Operative Steuerung der Informationssicherheit bei it@M durch das Cyber Security Center (CSC, im Aufbau).

Informationssicherheitsmanagement im RIT

- ISM aus IT-Sicht: Planung, Steuerung und Kontrolle der Informationssicherheit im RIT.
- Delegation der „Verantwortung für die IT-Sicherheit im RIT und bei it@M“ durch RIT-L / it@M - WL an Dr. Reeg.
- Bestellung von Frau Lenz (RIT-I A4) zur Informationssicherheitsbeauftragten des RIT.

Dezentrales Informationssicherheitsmanagement

- ISM aus Kundensicht: Planung, Steuerung und Kontrolle der Informationssicherheit in den Referaten / Eigenbetrieben gemäß den Vorgaben des stadtweiten Informationssicherheitsmanagements.
- Bestellung eines/einer Informationssicherheitsbeauftragten pro Ref / Eb.
- Keine Delegationen für das stadtweite Informationssicherheitsmanagement im IT-Referat.

Im Hinblick auf die eingangs genannten Perspektiven lassen sich die vier Verantwortungsbe-
reiche / Aufgabenfelder aktuell wie folgt kategorisieren:

	ISM stadtw.	ISM it@M	ISM RIT	ISM dez.
Personalrechtliche Perspektive				
Dienstaufsicht	RIT-I A4	RIT-I A4 / CSC	RIT-I A4	Ref/EB
Fachaufsicht	RIT-I A4	RIT-I A4	RIT-I A4	RIT-I A4
Verantwortungsperspektive				
Durchführungs- und Ergebnisverantwortung	RIT-I A4	RIT-I A4 / CSC	RIT-I A4	Ref/EB
Gesamtverantwortung (aus Sicht der LHM)	OB	it@M - WL	RIT - L	Ref/EB - L

Tabelle 1: IST-Situation personalrechtliche und Verantwortungsperspektive

Es wird deutlich, dass in den aktuellen Organisationsstrukturen lediglich die Fachaufsicht für das dezentrale Informationssicherheitsmanagement zentral im RIT verortet ist. Hierdurch fehlt die Möglichkeit der direkten, einheitlichen Steuerbarkeit der Mitarbeitenden im dezISM, wodurch es zu deutlichen Unterschieden in der Aufgabenausgestaltung, -priorisierung und -durchführung innerhalb der Ref / Eb kommt. Weiterhin kann auf diese Weise auch keine einheitliche und an den Bedarfen der LHM ausgerichtete Kompetenzentwicklung der Mitarbeitenden im Bereich der Informationssicherheit von zentraler Stelle aus durchgeführt werden.

3.2. Organisatorisches Zielbild

Um die im Stadtratsbeschluss adressierten Potentiale einer Zentralisierung erzielen zu können, müssen im Hinblick auf die dargestellte IST-Situation Anpassungen vorgenommen werden. Das resultierende Zielbild aus Sicht ISM stellt sich wie folgt dar:

	ISM stadtw.	ISM it@M	ISM RIT	ISM dez.
Personalrechtliche Perspektive				
Dienstaufsicht	RIT-I A4	RIT-I A4 / CSC	RIT-I A4	<i>RIT-I A4</i>
Fachaufsicht	RIT-I A4	RIT-I A4	RIT-I A4	RIT-I A4
Verantwortungsperspektive				
Durchführungs- und Ergebnisverantwortung	RIT-I A4	RIT-I A4 / CSC	RIT-I A4	<i>RIT-I A4</i>
Gesamtverantwortung (aus Sicht der LHM)	OB	it@M - WL	RIT – L	Ref/EB - L

Tabelle 2: Zielbild personalrechtliche und Verantwortungsperspektive

Im Wesentlichen ergeben sich zwei konkrete Änderungen im Hinblick auf die Aspekte der Dienstaufsicht und der Durchführungs- und Ergebnisverantwortung im dezISM. Gleichbleibend, jedoch unter der neuen Konstellation differenziert zu betrachten, ist der Aspekte der Gesamtverantwortung, der neben den beiden genannten Anpassungen im Folgenden ebenfalls beleuchtet wird.

Übergang der Dienstaufsicht zu RIT-I A4

Eine direkte disziplinarische Steuerung der Mitarbeitenden zur Erbringung der Aufgabe dezISM durch RIT-I A4 ist die Voraussetzung dafür, dass einheitliche Standards und damit Qualitäts- und Effizienzsteigerungen in der Aufgabendurchführung und -ausrichtung über alle Referate und Eigenbetriebe der Verwaltung hinweg erzielt werden können.

Weiterhin wird mit dem Übergang der Dienstaufsicht die Effektivität von Maßnahmenumsetzungen im Informationssicherheitsmanagement der LHM gesteigert, indem z. B. aktuelle Problemstellungen, wie etwa fehlende Stellvertretungen, durch organisationsbezogene Pooling-Ansätze bei RIT-I A4 aktiv und flexibel adressiert werden können.

Übergang der Durchführungsverantwortung für dezISM zu RIT-I A4

Die Durchführungs- und Ergebnisverantwortung der Aufgabe dezISM bei RIT-I A4 ist notwendig, um die formale Grundlage im Verwaltungskontext zu schaffen, dass diese Aufgabendurchführung ausschließlich durch Mitarbeitende erfolgen kann, die unter der Dienstaufsicht von RIT-I A4 stehen.

Verbleib der Gesamtverantwortung für dezISM bei den Ref / Eb (Leitungsebene)

Die Referate / Eigenbetriebe der LHM sind und bleiben immer „Herr ihrer Daten“ und tragen

entsprechend auch die Verantwortung dafür. Diese grundsätzliche Verantwortung ist per se nicht an andere Organisationseinheiten delegierbar. Somit gilt auch für die Informationssicherheit, dass die Verantwortung für die Sicherheit der Informationen eines Ref / Eb nicht delegierbar ist. Im Kontext der dargestellten Perspektiven bedeutet dies, dass die Gesamtverantwortung der Aufgabe dezISM im Ref / Eb verbleibt– und auch sinnvollerweise dort verbleiben muss.

Dieser Sachverhalt ist bereits in der aktuellen IST-Situation gegeben. Die Ausprägung der Gesamtverantwortung in den Ref / Eb wird dabei durch das Mittel der stadtweit verbindlichen IT-Sicherheitsvorgaben geschärft. Diese Vorgaben liefern einen einheitlichen Rahmen, der die zu erreichenden Ziele im Rahmen der Gesamtverantwortung konkretisiert. Gleichzeitig bleiben Entscheidungsmöglichkeiten auf Kundenseite bestehen, wie etwa im Bereich der Risikoübernahme bei IT-Projekten. Kontrollmöglichkeiten für die Leitungsebene der Ref / Eb im Rahmen der Gesamtverantwortung können durch festzulegende Reportingstrukturen durch die Mitarbeitenden im dezISM abgebildet werden.

3.3. Umsetzungsmaßnahmen und Synergiepotentiale

Für die Etablierung des dargestellten Zielbildes sind konkrete Maßnahmen im Rahmen des Umsetzungskonzepts zu realisieren. Diese werden im Folgenden erläutert.

Stellentransfer

Einen wesentlichen Effekt für die Zielsetzungen des Leistungsschnitts 2.0 entfaltet die direkte Steuerbarkeit der Mitarbeitenden im dezISM, die durch den Übergang der Dienstaufsicht zum gesamtstädtischen Informationssicherheitsmanagement im IT-Referat entsteht. Hierdurch können Aufgabendurchführungen und Vorgehensweisen über Referate und Eigenbetriebe hinweg standardisiert sowie Initiativen bzw. Positionen im Informationssicherheitsmanagement stadtweit einheitlich propagiert und effektiver umgesetzt werden.

Der Übergang der Dienstaufsicht zu RIT-I A4 erfolgt durch Stellentransfer der bisher in den Ref / Eb verorteten Stellen für dezentrale Informationssicherheitsbeauftragte zu RIT-I A4. Mit diesem Schritt werden für die Mitarbeitenden im dezentralen ISM dann auch direkte Schnittstellen innerhalb der IT-Organisation verfügbar, die im Zielbild der Zentralisierung eine effiziente Kommunikation in das IT-Service-Management (Kundenmanagement, Lösungsmanagement, Betrieb) unter aus Sicht des ISM einheitlichen Gesichtspunkten ermöglichen.

Änderung im Aufgabengliederungsplan

Um die Durchführungsverantwortung für die Aufgabe dezISM im IT-Referat zu verankern ist eine entsprechende Änderung im Aufgabengliederungsplan der LHM notwendig. Hierdurch wird sichergestellt, dass stadtweit einheitliche Strukturen entstehen und die Durchführung des dezentralen Informationssicherheitsmanagements ausnahmslos durch Mitarbeitende des IT-Referats wahrgenommen werden kann. Flankiert wird diese Verortung der Durchführungsverantwortung durch entsprechende Vorgaben im Rahmen des Regelwerks IT-Sicherheit der LHM, das stadtweit verbindlich gilt.

Zentrale Vorgaben zur Rolle des/der Informationssicherheitsbeauftragten

Im Rahmen des Regelwerks IT-Sicherheit ist zu hinterlegen, wie die Mitarbeitenden im Aufgabenbereich dezISM in ihrem Zuständigkeitsbereich (Ref / Eb) aus Organisationssicht

zugeordnet werden, welche direkten Ansprechpartner für sie im Rahmen ihrer Tätigkeiten bestehen, welche Befugnisse für die Durchführung ihrer Aufgaben notwendig sind und auf welche Weise diese Befugnisse geltend gemacht werden können.

Konkret sind die Mitarbeitenden hierbei in direkter Linie zur Geschäftsleitung in den jeweiligen Ref / Eb zu positionieren mit einer engen Einbindung in die Tätigkeiten des GPM sowie des Anforderungsmanagements. Weiterhin muss die Sichtbarkeit der Rolle des „Informationssicherheitsbeauftragten“, in der die Mitarbeitenden im dezISM in den jeweiligen Ref / Eb agieren, erhalten bleiben. Dies bezieht sich primär auf Kontakt- und Kommunikationsmöglichkeiten zu und mit den jeweiligen Fachbereichen, um insbesondere in Themenbereichen wie Security-Awareness oder den Umgang mit IT-Sicherheitsvorfällen effizient agieren zu können.

Um die Tätigkeiten im dezentralen Informationssicherheitsmanagement wahrnehmen zu können, müssen die Mitarbeitenden des IT-Referats über entsprechende Befugnisse in den jeweiligen Einheiten verfügen. Die Möglichkeit zur Verabschiedung von lokal geltenden Sicherheitsregularien ist ein diesbezügliches Beispiel. Auch hier sind im Regelwerk IT-Sicherheit entsprechende Vorgaben zu hinterlegen, die eine formale Abbildung der notwendigen Befugnisse ermöglichen, z. B. über Delegationen, Verfügungen oder entsprechende Bestellungen durch die Leitungsebene der jeweiligen Einheit.

Neben der Erteilung von Befugnissen ist für die Leitungsebene des jeweiligen Referats bzw. Eigenbetriebs auch eine Kontrollmöglichkeit über die aus dem dezISM erbrachten Ergebnisse notwendig, um den aus der Gesamtverantwortung resultierenden Anforderungen nachkommen zu können. In diesem Zusammenhang sind entsprechende Reportingstrukturen und-inhalte zu definieren und aufzubauen, über die eine angemessene Transparenz im Hinblick auf die Tätigkeiten im dezentralen Informationssicherheitsmanagement erzeugt wird.

Organisationsanpassungen im IT-Referat

Mit der Durchführungsverantwortung für dezISM und dem Übergang der Dienstaufsicht werden bei RIT-I A4 alle vier Verantwortungsbereiche im Informationssicherheitsmanagement der LHM zentral verortet. Bedingt durch die Anzahl an Stellen sind hierfür neue Abteilungsstrukturen zu schaffen. Weiterhin sind in diesem Rahmen neue Arbeitsplatzbeschreibungen zu erstellen, die dem Tätigkeitsprofil der „neuen“ Rolle des / der Informationssicherheitsbeauftragten entsprechen. Darüber hinaus sind die Einwertungen der Stellen zu vereinheitlichen und entsprechend anzupassen.

Die dargestellten Umsetzungsmaßnahmen stellen sicher, dass eine stadtweit einheitliche Organisationsstruktur für das dezentrale Informationssicherheitsmanagement etabliert wird. Diese Struktur stellt eine Voraussetzung dafür dar, dass einheitenübergreifende Standards definiert und Effizienzsteigerungen erzielt werden können. Neben den rein formal-organisatorischen Aspekten ist hierbei insbesondere auch die Verortung der neuen Rolle des Informationssicherheitsbeauftragten (Positionierung, Befugnisse, Präsenz) in den jeweiligen Einheiten von zentraler Bedeutung. Weiterhin bildet die einheitliche Organisationsstruktur die Grundlage für fachlich-inhaltliche Effizienzen, die als weiterer Bestandteil des Umsetzungskonzepts im folgenden Abschnitt erläutert werden.

4. Fachliche Perspektive

In der fachlichen Perspektive des Umsetzungskonzepts werden Effizienzpotentiale betrachtet, die sich bei einer standardisierten und einheitlichen Durchführung von Tätigkeiten im Rahmen der Aufgabe des dezentralen Informationssicherheitsmanagements ergeben. Im Ergebnis entsteht ein fachliches Zielbild, das diejenigen Teilaufgaben des dezentralen Informationssicherheitsmanagements enthält, deren Vereinheitlichung im stadtweiten Kontext besonders positive Effekte auf das IT-Sicherheitsniveau aufweisen.

Kapitel 4.1 erläutert den hierfür zu Grunde liegenden Ansatz, bevor in Kapitel 4.2 das fachliche Zielbild dargestellt wird. In Kapitel 4.3 werden abschließend die notwendigen Umsetzungsmaßnahmen für diesen fachlichen Teil des Konzepts dargestellt.

4.1. Konzeptueller Ansatz

Der grundlegende Ansatz aus Sicht des ISM besteht zunächst darin, die Durchführung bestimmte Tätigkeitsbereiche im dezISM aus stadtweiter Sicht zu vereinheitlichen. Die entsprechenden Tätigkeiten werden somit in jedem Ref / Eb in gleicher Weise durchgeführt, so dass sich eine Standardisierung im dezISM entwickelt.

Diese Standards können durch die direkte Steuerung im ISM der LHM (vgl. Kapitel 3) zentral verankert und stadtweit weiterentwickelt werden. Auf diese Weise können Effizienzen in der Durchführung sowie auch einheitliche Ebenen in der Umsetzungsqualität generiert werden.

Beispiele für geeignete Tätigkeitsbereiche im dezISM sind etwa vereinheitlichte Vorgehensweisen zur Einbindung und Mitwirkung als IT-Sicherheitsexperte in Projekten des jeweiligen Ref / Eb oder auch die Entwicklung, Bereitstellung und Anwendung von einheitlichen Formaten zur Sicherheitsdokumentation, für Reportings sowie für Awareness- und Schulungsmaßnahmen.

Als Rahmenbedingung für diesen Ansatz gilt, dass einheitenspezifische Gegebenheiten im dezentralen Informationssicherheitsmanagement im Rahmen der Effizienzgewinnung gewahrt bleiben. Aus realistischer Sicht werden somit nicht alle Tätigkeiten im dezISM stadtweit einheitlich ausgeprägt werden können.

Im Ergebnis der Standardisierung entstehen somit auch freie Kapazitäten, die dann in IT-Sicherheitsbereichen mit primärer Wirkung auf das stadtweite IT-Sicherheitsniveau zum Einsatz gebracht werden können. Beispiele hierfür sind das Risikomanagement IT-Sicherheit, das Security Event- und Incidentmanagement sowie das Security Control Management. In diesen IT-Sicherheitsprozessen bestehen durch die Verortung der Mitarbeitenden im IT-Referat zudem direkte Interaktionsmöglichkeiten mit den Betriebs- und Architektureinheiten sowie dem Cyber Security Center bei it@M, sodass auch in diesen Bereichen Effizienzsteigerungen in der Bearbeitung konkreter Prozessinstanzen zu erwarten sind.

Der dargestellte Ansatz schafft somit die Möglichkeiten, sowohl Effizienz- wie auch Qualitätssteigerungen im ISM zu generieren und damit sowohl einheitenspezifisch wie auch aus gesamtstädtischer Sicht das IT-Sicherheitsniveau der LHM zu entwickeln.

Gerade der letztgenannte Effekt auf das stadtweite IT-Sicherheitsniveau ist hierbei nicht zu vernachlässigen, da die heutige Personalsituation in den Verantwortungs- und Aufgabenbereichen des Informationssicherheitsmanagements mit stadtweiter Wirkung als unzureichend zu bezeichnen ist. Die hierdurch entstehenden Risiken für die Informationssicherheit der

LHM können durch den dargestellten Ansatz zwar nicht abgebaut, jedoch zumindest in Teilen adressiert werden.

4.2. Fachliches Zielbild

Auf der Grundlage des dargestellten Ansatzes werden im Folgenden die wesentlichen Aufgabenbereiche im dezentralen Informationssicherheitsmanagement dargestellt sowie im Hinblick auf ihre Eignung für die Schaffung von stadtweit einheitlichen Standards in den Ref / Eb bewertet.

Im Ergebnis entsteht ein Zielbild, dessen Inhalte als fachliche Komponenten des Umsetzungskonzepts zu verstehen sind. Diese Konzeptbausteine sind dann im Rahmen der Operationalisierung des Konzepts durch das ISM in der Organisation zu entwickeln und zu verankern.

Als Ausgangsbasis für die Bildung der fachlichen Konzeptbausteine fungieren die wesentlichen Teilaufgaben im dezentralen Informationssicherheitsmanagement, die durch die Rolle des / der Informationssicherheitsbeauftragten in den Ref / Eb wahrzunehmen sind.

In der folgenden Darstellung werden diese Teilaufgaben in 7 Bereiche gruppiert und auf geeigneter Abstraktionsebene dargestellt. Teilaufgaben, deren Beschreibung ein ✓ - Symbol voransteht, sind für eine Vereinheitlichung geeignet und als fachliche Konzeptbausteine des Zielbilds zu verstehen.

Ansprechpartner für Informationssicherheit

- ✓ Ansprechpartner für Mitarbeitende des Refs / Ebs in allen Fragen der Informationssicherheit
- Beratung und Steuerungsunterstützung der Leitung des Refs / Ebs in Fragen der Informationssicherheit des Refs / Ebs
- ✓ Vertreten der stadtweiten Informationssicherheitspositionen und -strategien in den Ref / Ebs
- ✓ Ansprechpartner für Steuerungseinheiten des Refs / Ebs mit Bezug zur Informationssicherheit, z. B. Datenschutz oder physische Sicherheit
- ✓ Vertreten der Belange der Informationssicherheit in allen relevanten Aktivitäten oder IT-Projekten des Ref / Ebs
 - Vertreten der Belange des Ref / Ebs im stadtweiten ISMS der LHM

Informationssicherheitsvorgaben und -ziele

- ✓ Erstellen der Umsetzungsvorschriften des Refs / Ebs
 - Erstellen referatsspezifischer Inhalte für die Umsetzungsvorschriften des Refs / Ebs
- ✓ Mitwirken bei der Konzeption und Umsetzung stadtweiter Informationssicherheitsvorgaben und deren Zielsetzungen

Informationssicherheitsereignisse und -vorfälle

- ✓ Mitwirken bei allgemeinen Informationssicherheitsereignissen und -vorfällen des Refs / Ebs

- Bearbeitung von referats- / eigenbetriebsindividuellen Informationssicherheitsereignissen und -vorfällen
- ✓ Stadtweite Zusammenarbeit bei Prävention, Detektion und Reaktion

Risikomanagement und IT-Sicherheitsmaßnahmen

- ✓ Sicherstellen bzw. Begleiten des Risikomanagements Informationssicherheit im Ref / Eb
- Controlling der referats- / eigenbetriebsindividuellen Informationssicherheitsmaßnahmen auf Wirksamkeit bzw. Anwendbarkeit im Ref / Eb
- ✓ Mitwirkung bei Konzeption und Umsetzung von stadtweit einheitlichen Informationssicherheitsmaßnahmen

Awareness- und Schulungsmaßnahmen zum Thema Informationssicherheit

- ✓ Unterstützung bzw. Konzeption stadtweit einheitlicher Schulungsmaßnahmen
- Umsetzung individueller Awareness- und Schulungsmaßnahmen für Mitarbeitende in Ref / Ebs
- Vertretung und Repräsentation der Informationssicherheit im referats- / eigenbetriebspezifischen Kontext

Reporting

- Erstellen regelmäßiger Berichte an die Leitungsebene des Res / Ebs
- ✓ Erstellen regelmäßiger Berichte an das ISM-Team für das stadtweite Reporting

Auditierung

- ✓ Durchführung von Auditierungen in Ref / Ebs
- ✓ Unterstützung des ISM-Teams bei Auditierungen

Die Auflistung der fachlichen Konzeptbausteine ist als nicht abschließend zu interpretieren. Im Hinblick auf die Umsetzung dieser Bausteine werden weiterführende Teilaspekte identifizierbar sein, die dann entsprechend auf ihre Eignung für eine stadtweite Standardisierung zu prüfen sein werden. In diesem Zusammenhang ist der Aufbau einer zentralen Wissensdatenbank zu den einzelnen Tätigkeitsbereichen notwendig, um die standardisierten Inhalte für alle Mitarbeitenden im Informationssicherheitsmanagement der LHM vorzuhalten und strukturiert fortzuschreiben.

4.3. Umsetzungsmaßnahmen

Um das fachliche Zielbild umzusetzen sind entsprechende Maßnahmen durchzuführen, die die fachlichen Konzeptbausteine (Kapitel 4.2) in der Sicherheitsorganisation der LHM etablieren und verankern. Diese Maßnahmen werden im Folgenden dargestellt.

Inhaltliche Entwicklung der stadtweiten Standards

Die fachlichen Konzeptbausteine müssen dem Zielbild entsprechend inhaltlich ausgestaltet werden. Hierzu sind entsprechende Workshops über alle Ref /Eb notwendig, um die bestehenden Gemeinsamkeiten und Unterschiede in den referatsspezifischen Vorgehensweisen

zu identifizieren und im Anschluss geeignet zu vereinheitlichen.

Fortschreibung und Verankerung der Standards im ISM der LHM

Hierbei geht es einerseits um die kontinuierliche Anpassung bzw. Fortschreibung der Standards sowie auch um die Steuerung ihres „Roll-Outs“ in allen Ref /Eb. Wesentliche Voraussetzung für Effizienzen in diesem Bereich ist der in Kapitel 3 als Umsetzungsmaßnahme ausgewiesene Übergang der Dienstaufsicht zu RIT-I A4.

Ausbildung von Tätigkeitsprofilen für dezentrale Informationssicherheitsbeauftragte

Die Tätigkeitsprofile von Mitarbeitenden im dezentralen Informationssicherheitsmanagement erfahren durch die angestrebten Standardisierungen erhebliche Änderungen im Hinblick auf Aufgabeninhalte, Priorisierungen und Vorgehensweisen. Diese Änderungen, auch bedingt durch Perspektiven- und Kulturwechsel, müssen in Form von klar umrissenen Tätigkeitsprofilen adressiert werden, um eine effektive und effiziente Durchführung des dezentralen Informationssicherheitsmanagements gewährleisten zu können. Darüber hinaus sind in diesem Zusammenhang individuelle Kompetenzentwicklungen einzuplanen und zu veranlassen.

Aufbau von Teams mit spezifischem Expertenwissen

Für spezifische Themenstellungen bietet es sich an, dass entsprechende Kompetenzen und Spezialwissen nicht über alle Mitarbeitenden hinweg aufgebaut werden, sondern im Rahmen von dedizierten Teams zielgerichtet entwickelt werden (Expertenteams). Ein Beispiel hierfür ist etwa der Bereich der Auditierung, der durch ein spezifisches Team von Experten einheitenübergreifend übernommen werden kann. Vor diesem Hintergrund sind entsprechende Themenbereiche zu identifizieren und Teams zu bilden, die den jeweiligen Aufgabenbereich dann ohne Fokus auf bestimmte Einheiten konzeptuell entwickeln bzw. umsetzen. Auch hier sind Maßnahmen zu individuellen Kompetenzentwicklungen einzuplanen und durchzuführen.

Mit der Umsetzung der dargestellten Maßnahmen wird das fachliche Zielbild des vorliegenden Konzepts umgesetzt. Teile dieser Maßnahmen sind kontinuierlich durchzuführen und müssen daher in der Linienorganisation bei RIT-I A4 verankert werden. Ein Beispiel hierfür sind etwa die stadtweiten Standards im dezentralen Informationssicherheitsmanagement, deren Fortschreibung dann als Linienaufgabe zu etablieren ist.

5. Pilotierung des Umsetzungskonzepts im MOR

Mit Beschlussfassung des Stadtrats vom 28.07.2021 wurde festgelegt, die in den Kapiteln 3 und 4 beschriebenen Inhalte des Umsetzungskonzepts für den Bereich Informationssicherheit im Mobilitätsreferat zu pilotieren.

Auf Grund des eng gefassten Zeitrahmes können im Hinblick auf die personalrechtliche bzw. organisationsbezogene Perspektive des Umsetzungskonzepts an dieser Stelle keine Aussagen getroffen werden. Die Durchführung von Stellentransfers, Änderungen im Aufgabengliederungsplan oder auch die Schaffung von neuen Organisationsstrukturen in Verbindung mit neuen Tätigkeitsprofilen und damit auch Perspektiven für Mitarbeitende in der Informationssicherheit sind im Laufe eines Quartals nicht pilotierbar.

Es verbleibt somit die fachliche Perspektive des Umsetzungskonzepts, über die eine mögliche Verprobung fachlicher Konzeptbausteine im MOR erfolgen kann. Konkret geht es in

diesem Zusammenhang also darum, die Aufgaben des dezentralen Informationssicherheitsmanagements im Mobilitätsreferat durch eine / einen Mitarbeitende*n im Informationssicherheitsmanagement des IT-Referats abzubilden und durchführen zu lassen.

Da zum aktuellen Zeitpunkt keine Stellenschaffungen bzw. -besetzungen möglich und im IT-Referat keine freien Kapazitäten vorhanden sind, werden externe Kapazitäten für diesen Verantwortungsbereich im ISM des IT-Referats zugeschaltet. Ein entsprechender Abruf bei externen IT-Dienstleistern läuft zum Zeitpunkt der Konzepterstellung.

Sobald entsprechende Kapazitäten zur Verfügung stehen, werden seitens RIT-I A4 alle Konzeptbausteine (vgl. Kapitel 4.2) für das Mobilitätsreferat als Piloteinrichtung übernommen.

Abschließend muss festgehalten werden, dass tatsächliche Synergien und qualitative Effizienzsteigerungen im dezentralen Informationssicherheitsmanagement erst dann generiert werden können, wenn das Umsetzungskonzept in allen Referaten und Eigenbetrieben Anwendung findet. Im Bereich der Informationssicherheit geht es im Sinne der Beschlussfassung schließlich nicht um die Reduktion vorhandener Doppelstrukturen, sondern in erster Linie um die Schaffung von stadtweit einheitlichen Standards im dezentralen Informationssicherheitsmanagement. Erst danach können Effizienzen in den vereinheitlichten Aufgabendurchführungen erzeugt werden, deren Effekte dann zu einer Steigerung des stadtweiten Informationssicherheitsniveaus genutzt werden können.