Information über Beschluss mit Folgekosten

Hinweise: Bitte jedes der unten stehenden Felder befüllen und maximal zwei bis drei Seiten!

Referat: RIT	Haupt-/Abteilung(en) (Bereich): RIT - I	betroffene Referate: alle
Öffentliche BV: ☒	Nicht-Öffentliche BV: ☒	Federführung: RIT
Arbeitstitel geplanter Beschluss: IT-Sicherheit bei der LHM		

1. Aufgabe

1.1 Kurze Beschreibung der Aufgabe:

Mit der Reorganisation der IT einher geht die Umstrukturierung der IT-Sicherheit der LHM. In diesem Zusammenhang wird bei RIT-I eine neue Abteilung „IT-Sicherheitsmanagement“ (ISM) geschaffen, bei it@M wird ein "Cyber Security Center" (CSC) aufgebaut.

Der Abteilung ISM im RIT werden neben den im RIT bereits bestehenden Aufgaben zur IT-Sicherheit, z. B. die IT-Sicherheitsstrategie oder das stadtweite Informationssicherheits-Managementsystem (ISMS), weitere Aufgaben zugeordnet. Im Zielbild werden neben dem stadtweiten IT-Sicherheitsmanagement ebenfalls das IT-Sicherheitsmanagement für das RIT sowie das IT-Sicherheitsmanagement von it@M in dieser Abteilung zusammengeführt.

Die Aufgaben des bei it@M aufzubauenden Cyber Security Centers sind im Vergleich etwas technischer ausgestaltet. Sie beziehen sich im Kern darauf, das IT-Sicherheitsniveau der LHM durch präventive Gefährdungsanalysen, konsistente IT-Sicherheitsarchitekturen sowie durch koordinierte Reaktionen auf eingetretene Schadwirkungen zu optimieren. Um diese Aufgaben im Rahmen des IT-Sicherheitsmanagements umzusetzen ist geplant, das CSC in Form der drei Bereiche IT-Sicherheitsarchitektur, Security Operation Center (SOC) und Offensive Security aufzubauen.

Die beantragten Mittel bilden die Grundlage für diese Reorganisation und damit für die Weiterentwicklung des IT-Sicherheitsmanagements der LHM sowie für die Etablierung des Cyber Security Centers bei it@M.

1.2 Aufgabenart

Pflichtaufgabe ☒	freiwillige Aufgabe ☐	bürgernahe Aufgabe ☐
Daueraufgabe ☒	zeitlich begrenzte Aufgabe ☐	

Kurze Begründung:

Die Relevanz der IT-Sicherheit für die LHM und insbesondere ihre Bedeutung für die Digitalisierung ist unumstritten. Dies unterstreichen nicht zuletzt die Aussagen des IT-Planungsrats, die in der "Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung" getroffen werden. Darüber hinaus ist die LHM mit ihren kritischen Infrastrukturen über die BSI-Kritisverordnung (BSI-KritisV) verpflichtet, entsprechende Standards in der IT-Sicherheit einzuhalten. Zusätzlich wird im Bayerischen E-Government-Gesetz (BayEGovG, Art. 11 Abs. 1) grundsätzlich gefordert, dass die IT-Sicherheit informationstechnischer Systeme sicherzustellen ist.

Diese gesetzlich verankerten Anforderungen verdeutlichen, dass die Gewährleistung von IT-Sicherheit in heutigen Zeiten eine der Kernaufgaben der öffentlichen Verwaltung darstellt. Bürgerinnen und Bürger, Unternehmen und weitere Partner erwarten zu Recht von der LHM, dass ihre Informationen bei der Verwaltung mit einem ausreichenden Schutzniveau verarbeitet und gespeichert werden.

Die LHM kann diese Anforderungen nur umsetzen, indem die IT-Sicherheit der LHM konsequent geplant, gesteuert und auch kontrolliert wird. Dies betrifft als Pflicht- sowie als Daueraufgabe sowohl den Bereich des (strategischen) IT-Sicherheitsmanagements im RIT (ISM) wie auch die taktischen und operativen Aspekte der IT-Sicherheit, die bei it@M verankert sind (CSC).

1.3 Auslöser des Mehrbedarfs

inhaltlich/ qualitative Veränderung der Aufgabe ☒	neue Aufgabe ☒	quantitative Aufgabenausweitung ☒

Kurze Erläuterung:

Mit der Umstrukturierung der IT-Sicherheit (Aufgabenverteilung und -bündelung in ISM und CSC) werden insbesondere zwei wesentliche Zielsetzungen adressiert. Zum einen folgt dieser Ansatz notwendigerweise den aktuellen Reorganisationen in der IT (Gründung RIT, Leistungsschnitt, Programm neoIT). Er stellt sicher, dass die IT-Sicherheit auch in den neuen organisatorischen Strukturen und Prozessen in der IT in allen relevanten Bereichen und in effizienter Art und Weise verankert ist. Des Weiteren wird durch die Etablierung des CSC ein wesentliches Bindeglied geschaffen zwischen dem IT-Sicherheitsmanagement im RIT und dem operativen Betrieb von IT-Sicherheitstechnologien bei it@M.

Auf diese Weise wird eine einheitliche IT-Sicherheitsarchitektur realisiert, die eine kontinuierliche Prüfung und Entwicklung des IT-Sicherheitsniveaus (proaktiv) sowie ein konsistentes Management von IT-Sicherheitsvorfällen (reaktiv) ermöglicht. Beide Punkte stellen wesentliche Voraussetzungen dar, um die IT-Sicherheit in der LHM auch zukünftig gewährleisten zu können. Darüber hinaus bilden diese Aspekte die Grundlage dafür, wenn perspektivisch gesehen eine IT-Sicherheitszertifizierung von relevanten Teilbereichen von it@M angestrebt wird.

Um diese Zielsetzungen zu erreichen, sind neue Aufgabenstellungen anzugehen, die im strategisch-konzeptionellen Umfeld angesiedelt sind - sowohl im Hinblick auf den Aufbau des CSC wie auch in Bezug auf die Weiterentwicklung zentraler IT-Sicherheitsprozesse. Im Ergebnis werden die Grundlagen geschaffen, um gesetzlichen Anforderungen im Hinblick auf die IT-Sicherheit auch weiterhin erfüllen zu können sowie um die Einbindung der IT-Sicherheit in alle IT-Lösungen der LHM effizient und angemessen zu gestalten.

Vor diesem Hintergrund sollen im Jahr 2020 mit zusätzlichen Ressourcen sowie mit externer Unterstützung insbesondere die folgenden Themen im Bereich der IT-Sicherheit der LHM adressiert werden.

<u>Etablierung einer zentralen Softwareplattform für das Management der IT-Sicherheit</u>

Im Kontext der IT-Sicherheit besteht gerade in großen Organisationen wie der LHM eine hohe Themenkomplexität. Diese erstreckt sich von organisatorischen und regulatorischen Aspekten, über IT-Sicherheitsprozesse und -architekturen bis hin zu rein technischen Aspekten und konkreten IT-Sicherheitsmaßnahmen.

Um diese Komplexität im Sinne des Managements handhabbar zu machen und um die dafür notwendige Zusammenarbeit zwischen ISM und CSC effizient zu gestalten, bedarf es einer integrierten Softwareplattform. Solche Systeme werden in der Regel als browserbasierte Anwendungen ausgeprägt und unterstützten die gemeinschaftliche Bearbeitung notwendiger Aufgabenbereiche, wie z. B. die Nachverfolgung von IT-Sicherheitsvorfällen, die Dokumentation von IT-Sicherheitsaudits oder die einheitenübergreifende Planung von IT-Sicherheitsmaßnahmen.

Die Etablierung einer solchen Softwareplattform bei it@M wird über ein für 2020 geplantes IT-Vorhaben realisiert, das auf 5 Jahre gerechnet Sachmittel in Höhe von EUR 1,5 Mio erfordern wird (Beschaffung, Lizenzkosten, Betrieb). Hiervon fallen in 2020 Aufwände in Höhe von EUR 350.000 an.

<u>Verankerung des Risikomanagements IT-Sicherheit bei RIT-I</u>

Das Management von Risiken stellt ein zentrales Paradigma im Rahmen des IT-Sicherheitsmanagements dar und ist ein wesentlicher Bestandteil der Entwicklung und des Lifecycles von IT-Services bei der LHM. Eine Risikoanalyse im Bereich IT-Sicherheit ist in jedem IT-Vorhaben der LHM verbindlich vorgeschrieben. Mit der Reorganisation des IT-Sicherheitsmanagements soll der diesbezüglich etablierte IT-Sicherheitsprozess neu strukturiert werden und im Sinne der neuen Rolle der IT eine Zentralisierung im RIT erfahren. Auf diese Weise werden dringend notwendige Effizienzsteigerungen erzielt,

die zum Beispiel auch dazu führen werden, die Durchlaufzeiten in der IT-Lösungsentwicklung zu verbessern.

Heute werden die entsprechenden Aufgabenbereiche eines Risikomanagers bei it@M durch vier externe Mitarbeiter übernommen. Durch beauftragungsbedingte Wechsel dieses Personals kommt es unvermeidlich zu Know-how Abflüssen und Mehraufwänden in Bezug auf das Anlernen neuen Personals. Es ist aus strategischer Sicht daher zielführend, Kapazitäten und entsprechendes Know-how für einen solchen elementaren Aufgabenbereich in der IT-Sicherheit intern aufzubauen. Weiterhin ist es notwendig, die entsprechenden Aufgaben an zentraler Stelle zu verankern, um Effizienzsteigerungen im Rahmen der stadtweiten Steuerung des Risikomanagements IT-Sicherheit zu erzielen.

Vor diesem Hintergrund werden in Summe 6 dauerhafte Stellen für Risikomanager im RIT benötigt. 4 dieser Stellen fungieren als Ersatz für die aktuell eingesetzten externen Mitarbeiter. Zusätzlich werden 2 weitere Stellen benötigt, da auf Grund von Kapazitätsengpässen bereits heute schon nicht alle notwendigen Risikoanalysen in den IT-Vorhaben der LHM durchgeführt werden können. Insbesondere im Kontext der Digitalisierung ist davon auszugehen, dass diese Fallzahlen in Zukunft weiter steigen werden. Eine Erhöhung der Kapazitäten um 50% ist daher unerlässlich, um alle IT-Vorhaben der LHM aus IT-Sicherheitsgesichtspunkten zukünftig ausreichend abdecken zu können.

Bis die Besetzung der 6 Stellen vollzogen werden kann, sind die Aufgaben des Risikomanagements IT-Sicherheit in 2020 durch die Zuschaltung externer Kapazitäten abzudecken. Hierfür fallen in Summe Aufwände in Höhe von EUR 1.584.000 (1.320 PT) an.

<u>Etablierung des Cyber Security Centers</u>

Wie eingangs in Kapitel 1.1 beschrieben, sehen die Planungen vor, die Aufgabenbereiche des CSC in drei Segmente zu unterteilen.

Im Bereich „IT-Sicherheitsarchitektur“ werden dabei Beratungs- und Konzeptionsleistungen zur IT-Sicherheitsarchitektur der LHM angesiedelt sowie die Entwicklung von fachlichen Roadmaps zum Einsatz von IT-Sicherheitstechnologien.

Der Bereich „Security Operation Center“ adressiert das operativ orientierte zentrale IT-Sicherheitsmonitoring, das sicherheitsrelevante Meldungen und Ereignisse aus der gesamten IT-Infrastruktur zentral aufnimmt und analysiert. Anhand dieser Analyseergebnisse werden dann standardisierte Verfahren zur Behandlung von IT-Sicherheitsvorfällen umgesetzt.

Im Rahmen des Bereichs „Offensive Security“ sind schließlich Aufgaben angesiedelt, die sich mit der proaktiven Erkennung von Schwachstellen in der IT-Infrastruktur der LHM, z. B. durch Penetration Tests, sowie mit deren Management befassen.

Für die Abdeckung der skizzierten Aufgabenbereiche werden dauerhaft 10 Stellen benötigt, die bei it@M im Cyber Security Center anzusiedeln sind. Im Detail werden im Bereich IT-Sicherheitsarchitektur 2 IT-Ingenieure IT-Sicherheit benötigt, im Bereich Security Operation Center 5 IT-Sicherheitsanalysten sowie im Bereich Offensive Security 3 IT-Ingenieure IT-Sicherheit.

Aus Sicht des RIT als Auftraggeber für die Etablierung des CSC ergibt sich auf Basis des gemittelten Verrechnungssatzes für IT-Stellen bei it@M für das Jahr 2020 ein Mittelbedarf in Höhe von EUR 2.061.000.

Die Zeitspanne bis zu der Besetzung der Stellen muss weiterhin durch externe Kapazitäten abgedeckt werden. Hierfür wird für das Jahr 2020 ein Bedarf an externen Dienstleistern bei it@M in Höhe von 660 PT (EUR 792.000) prognostiziert.

<u>Werkzeugunterstützung für die Behandlung von IT-Sicherheitsvorfällen</u>

Ein schnelles und wirksames Management von IT-Sicherheitsvorfällen ist ein zentrales reaktives Element im Rahmen der IT-Sicherheit. Hierbei geht es um die effiziente Behandlung von Ereignissen, die die z. B. die Vertraulichkeit von Informationen kompromittiert haben oder sie beeinträchtigen könnten. Dieser operative Aufgabenbereich ist im Security Operation Center des CSC zu etablieren und umfasst sowohl die Reaktion auf konkrete technische Gefährdungen, wie z. B. Erpressungstrojaner, wie auch den Umgang mit abstrakten Bedrohungslagen, wie z. B. Datenleaks oder globalen Phishingwellen.

Um die hierfür notwendigen IT-Sicherheitsprozesse standardisiert zu etablieren und auch in der kon-

kreten Durchführung effizient abarbeiten zu können, ist eine Werkzeugunterstützung für die Mitarbeiterinnen und Mitarbeiter im Security Operation Center erforderlich. Über dieses Werkzeug werden IT-Sicherheitsvorfälle strukturiert erfasst und verarbeitet sowie notwendige Gegenmaßnahmen eingeleitet und gesteuert. Zusätzlich können Warnmeldungen auch aus externen Quellen zentral erfasst und bearbeitet werden.

Für die Einführung des Werkzeugs entstehen im Betrachtungszeitraum von 5 Jahren Gesamtkosten in Höhe von EUR 300.000. Auf das Jahr 2020 entfällt davon ein Mittelbedarf in Höhe von EUR 200.000.

2. Finanzielle Auswirkungen	
2.1 Zahlungen gesamt	**2020 - 2024**
2.1.1 Gesamteinzahlungen konsumtiv	0 €
2.1.2 Gesamtauszahlungen konsumtiv	6.237.000 € Sachkosten 1.620.000 € Personalkosten
2.1.3 Gesamteinzahlungen investiv	0 €
2.1.4 Gesamtauszahlungen investiv	0 €
2.2 konsumtiv	**Planjahr 2020**
2.2.1 Einzahlungen	**0 €**
2.2.1.1 Zuwendungen und allgemeine Umlagen	0 €
2.2.1.2 Sonstige Transfereinzahlungen	0 €
2.2.1.3 Öffentlich-rechtliche Leistungsentgelte	0 €
2.2.1.4 Privatrechtliche Leistungsentgelte	0 €
2.2.1.5 Kostenerstattungen und Kostenumlagen	0 €
2.2.1.6 Sonstige Einzahlungen aus lfd. Verwaltungstätigkeit	0 €
2.2.2 Auszahlungen	**5.183.800 €**
2.2.2.1 Personalauszahlungen	180.000 €
2.2.2.2 Auszahlungen für Sach- und Dienstleistungen (ohne Arbeitsplatzkosten)	4.987.000 €
2.2.2.3 Arbeitsplatzkosten	16.800 €
2.2.2.4 Transferauszahlungen	0 €
2.2.2.5 Sonstige Auszahlungen aus lfd. Verwaltungstätigkeit	0 €
2.3 investiv	**Planjahr 2020**
2.3.1 Einzahlungen	0 €
2.3.2 Auszahlungen	0 €

3. Erforderliche Stellenbemessung gem. Leitfaden ist erfolgt?	☒ ja	☐ nein

4. Geltend gemachter Bedarf			
geltend gemachter Stellenmehrbedarf für das Planjahr	VZÄ	davon befristet VZÄ	QE, FR
	6 Risikomanager IT-Sicherheit	-	E13, IT
geltend gemachter Stellenmehrbedarf für den Gesamtzeitraum	VZÄ	davon befristet VZÄ	QE, FR
	6 Risikomanager IT-Sicherheit	-	E13, IT
bereits für die Aufgabe eingesetzt	VZÄ	davon befristet VZÄ	QE, FR
	0		

5. zusätzlicher Büroraumbedarf		
5.1 Kann der geltend gemachte Stellenbedarf in den vorhandenen Bestandsflächen des Referats untergebracht werden?		
☐ ja	☒ nein	☐ teilweise
5.2 Falls „nein“ / „teilweise“ ausgewählt wurde: Für wie viele der in Ziffer 3 gemeldeten VZÄ wird Büroflächenbedarf ausgelöst? 6 VÄZ		

6. Refinanzierung	
6.1 des geltend gemachten Stellenbedarfs:	
Art:	Höhe in %:
6.2 des geltend gemachten Sachmittelbedarfs:	
Art:	Höhe in %: