



Protokollauszug vom

03.12.2025

Departement Finanzen / Informatikdienste:

ICT-Risikomanagement – Konzept und Implementierung

IDG-Status: öffentlich

Beschluss-Nr.: 2025/992

Der Stadtrat hat beschlossen:

1. Das Konzept zum neuen stadtweiten ICT-Risikomanagement wird gemäss Beilage 1 genehmigt.
2. Das Departement Finanzen, Informatikdienste, wird beauftragt, das neue ICT-Risikomanagement zu implementieren.
3. Mitteilung an: alle Departemente; Stadtkanzlei; Departement Finanzen, Informatikdienste.

Vor dem Stadtrat

Der Stadtschreiber:



MOXIS



A. Simon

Begründung:

1. Ausgangslage

Die zunehmende Digitalisierung städtischer Aufgaben führt zu erheblichen Risiken im Bereich der Informations- und Kommunikationstechnologien (ICT). Vor diesem Hintergrund hat der Stadtrat im Legislaturprogramm 2022–2026 unter dem Schwerpunkt «Leistungsfähige Verwaltung» das Ziel formuliert, die Cybersecurity durch ein systematisches ICT-Risikomanagement zu stärken.

In den Departementen und Bereichen der Stadt Winterthur gibt es unterschiedliche Ansätze im Umgang mit Risikomanagement. Seit Ende 2024 erarbeitet die Versicherungsfachstelle eine einheitliche Sichtweise, die bestehende Ansätze auf Departements- sowie gesamtstädtischer Ebene zusammenführt. Eine detaillierte Analyse der einzelnen ICT-Risiken – inklusive möglicher finanzieller und nicht-finanzieller Auslöser und Auswirkungen – liegt aktuell noch nicht vor.

Bei der Einführung neuer IT-Anwendungen führen die zuständigen Bereiche zusammen mit den Informatikdiensten (IDW) eine Schutzbedarfsanalyse (SBA) durch. Fachpersonen bewerten die spezifischen Prozesse der Anwendung hinsichtlich der Verfügbarkeit, Integrität, Existenz und Vertraulichkeit von Daten. Die SBA identifiziert Risiken und definiert technische sowie organisatorische Massnahmen zur Minimierung dieser Risiken.

Einheitliche Kriterien zur Erhebung, Beschreibung, Bewertung und Kontrolle von ICT-Risiken sowie eine bereichs- und departementsübergreifende Gesamtsicht fehlen bislang.

Die vom Parlament bewilligte Stelle der «ICT-Risikomanager:in» zur Erstellung und Führung des stadtweiten ICT-Risikomanagements wurde per 1. Mai 2025 besetzt. Die Fachperson leitet und unterstützt die Bereiche gezielt im Umgang mit ICT-Risiken, schafft eine konsolidierte Übersicht dieser Risiken auf Bereichs- und Departementsebene und stärkt damit die Steuerungsfähigkeit der Stadt.

2. Ziele

Das stadtweite ICT-Risikomanagement wird ein eigenständiger Bestandteil des gesamtstädtischen Risikomanagements, das vom Stadtrat am 4. Dezember 2024 genehmigt wurde (SR.24.812-1). Im Antrag wird bewusst auf die Darstellung von Varianten verzichtet, da sich der Aufbau und die Konzeption des ICT-Risikomanagements direkt an den Vorgaben und Strukturen des gesamtstädtischen Risikomanagements orientieren.

Die Einführung des stadtweiten ICT-Risikomanagements verfolgt folgende Ziele:

- Systematische und periodische Identifikation, Analyse, Bewertung, Behandlung und Überwachung von ICT-Risiken
- Einheitlicher Ansatz zur Erfassung und Beschreibung von ICT-Risiken und Massnahmen
- Konsolidierte Sicht auf bestehende ICT-Risiken pro Bereich und Departement
- Anbindung an das gesamtstädtische Risikomanagement, inklusive Risikoberichterstattung
- Stärkung der Resilienz der städtischen Bereiche gegenüber ICT-bezogenen Bedrohungen

3. Grundlagen des ICT-Risikomanagements

Risikomanagement ist eine Methode zur Identifikation von Ereignissen oder Umständen, die für die Erreichung der gesetzten Ziele relevant sind.

Im Rahmen des übergreifenden Risikomanagements konzentriert sich das ICT-Risikomanagement auf die spezifische Identifikation, Analyse und Bewertung von Risiken im Zusammenhang mit Informationen, Technologien, Systemen und Anwendungen. Dabei werden ICT-Risiken zunehmend ganzheitlich als Informationsrisiken verstanden.

Informationsrisiken bedrohen die Verfügbarkeit, Integrität, Existenz und Vertraulichkeit von Informationen. Sie entstehen nicht nur durch IT-Systeme, sondern auch durch Prozesse, organisatorische Strukturen oder menschliches Verhalten. Im Unterschied zu IT-Risiken beziehen sie sich auf Informationen insgesamt – unabhängig von der verwendeten Technologie.

Das ICT-Risikomanagement der Stadt Winterthur orientiert sich am internationalen Standard ISO/IEC 27005:2022, der Leitlinien für das Risikomanagement der Informationssicherheit bietet.

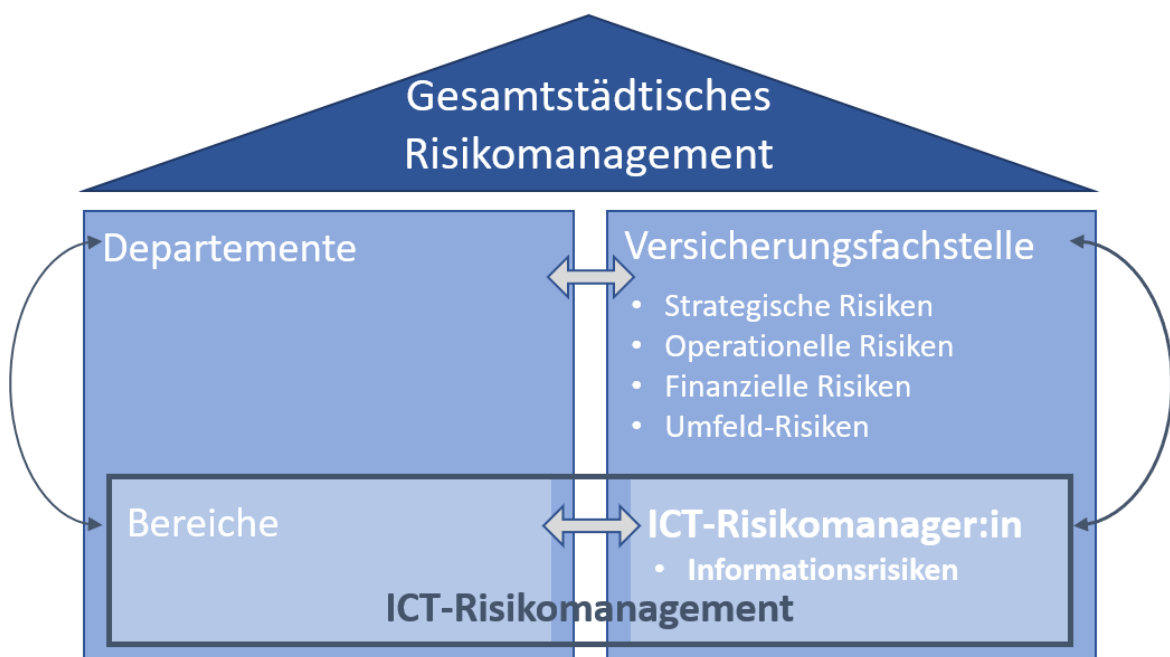
4. Einbettung in das gesamtstädtische Risikomanagement und Abgrenzung zum Business Continuity Management (BCM)

Das stadtweite ICT-Risikomanagement ordnet sich als eigenständiger Teil in das gesamtstädtische Risikomanagement ein. Es verwendet denselben Risikotypenkatalog und die gleichen Bewertungsmethoden. Um Synergien optimal zu nutzen und Überschneidungen zwischen der Versicherungsfachstelle und der ICT-Risikomanager:in zu vermeiden, stehen beide Funktionen in regelmässigem Austausch.

Die Versicherungsfachstelle ermittelt die wesentlichen Risiken in Risikomanagement-Workshops mit den Departementen, an denen auch die ICT-Risikomanager:in teilnimmt. Zusätzlich führt die ICT-Risikomanager:in eigenständige Risikobeurteilungen mit den einzelnen Bereichen durch.

Das Business Continuity Management (BCM) steht in engem Zusammenhang mit dem ICT-Risikomanagement. Es sorgt dafür, dass kritische städtische Aufgaben und Dienstleistungen im Ereignisfall rasch wieder aufgenommen werden. BCM ist eine reaktive Massnahme für bestimmte Gefahren, die im Risikomanagement ermittelt wurden. Wenn BCM-Massnahmen, wie Wiederherstellungspläne, das ICT-Risikomanagement betreffen oder daraus abgeleitet werden, erfolgt eine Abstimmung zwischen beiden Bereichen.

Das folgende Bild zeigt den Aufbau und das Zusammenspiel der Organisationseinheiten im Risikomanagement der Stadt Winterthur:



5. Risikoeinheiten

Die Bereiche der Stadt Winterthur fungieren als eigenständige Risikoeinheiten. Für jede Risikoeinheit werden die Informationsrisiken, deren Auswirkungen und Massnahmen in einem Risiko-Register dokumentiert. Die Ergebnisse werden auf Departementsebene zusammengefasst und in den gesamtstädtischen Risikobericht aufgenommen.

Die rund 40 Bereiche, die direkt dem Stadtrat unterstellt sind, werden als Risikoeinheiten definiert. Ausgenommen sind die Aufsichtsbehörden (Datenschutzstelle, Finanzkontrolle, Ombudsstelle), die Parlamentsdienste, die einzelnen Volksschulen, die Schulpflege, die Sozialhilfebehörde und die Pensionskasse der Stadt Winterthur.

Diesen städtischen Organisationseinheiten steht im Rahmen der verfügbaren Ressourcen der ICT-Risikomanager:in (IDW) die Möglichkeit zur Teilnahme am ICT-Risikomanagement offen.

6. Organisation, Rollen und Verantwortlichkeiten

Das ICT-Risikomanagement umfasst die städtischen Bereiche sowie die ICT-Risikomanager:in. Die Bereiche verwalten und verantworten ihre ICT-Risiken und Massnahmen, die teilweise bereits in den Schutzbedarfsanalysen (SBA) dokumentiert sind. Die ICT-Risikomanager:in unterstützt die systematische Erfassung und Bearbeitung der Risiken und definiert die Prozesse, Standards sowie Methoden für das stadtweite ICT-Risikomanagement.

Die wichtigsten Rollen im stadtweiten ICT-Risikomanagement sind:

- **ICT-Risikomanager:in**
Verantwortlich für die Organisation sowie die fachliche und methodische Führung.
- **Risikoeigner:in (i.d.R. Stufe Geschäftsleitung)**
Verantwortlich für die Identifikation und Behandlung der Risiken. Verfügt über die notwendigen Kenntnisse und Kompetenzen zur Risikosteuerung. Hat Führungs- und Fachverantwortung im jeweiligen Bereich. Kann die Umsetzung der Massnahmen an eine Risikoverantwortliche delegieren, die Verantwortung bleibt jedoch bestehen.
- **Risikoverantwortliche**
Verantwortlich für die konkrete Umsetzung der definierten Massnahmen.
- **Ansprechperson**
Kontaktperson zwischen der ICT-Risikomanager:in und dem jeweiligen Bereich.

Der ICT-Risikomanagement-Prozess findet mindestens alle zwei Jahre statt. Die ICT-Risikomanager:in plant, organisiert und führt die Risikobeurteilungen durch. Die Bereiche bereiten sich darauf vor, indem sie potenzielle Risiken prüfen, bestehende Massnahmen evaluieren und aktiv an den Workshops zur Risikobeurteilung teilnehmen.

7. Aufwand und Kosten

Der geschätzte Durchschnittsaufwand ergibt sich aus der Tabelle in Beilage 1:

Involvierte Stellen	Periodizität	Aufwand in Tagen
ICT-Risikomanager:in (pro Bereich)	Einmalig	1.4 d
ICT-Risikomanager:in (pro Bereich)	Mindestens alle 2 Jahre wiederkehrend	3.4 d
ICT-Risikomanager:in (pro Departement)	Mindestens alle 2 Jahre wiederkehrend	3.0 d
Risikoeigner:innen = Führungs- und Fachverantwortliche	Einmalig	0.2 d pro Person
Risikoeigner:innen = Führungs- und Fachverantwortliche	Mindestens alle 2 Jahre wiederkehrend	0.7 d pro Person
Ansprechperson (pro Bereich)	Einmalig	0.4 d
Ansprechperson (pro Bereich)	Mindestens alle 2 Jahre wiederkehrend	0.3 d
Risikoverantwortliche	Mindestens alle 2 Jahre wiederkehrend	0.2 d pro Person
Versicherungsfachstelle (pro Departement)	Mindestens alle 2 Jahre wiederkehrend	1.5 d

Durch die gezielte Führung und methodische Unterstützung der ICT-Risikomanager:in beträgt der wiederkehrende Aufwand, der mindestens alle zwei Jahre anfällt, pro beteiligte Person weniger als einen Arbeitstag. Der Aufwand pro Bereich hängt von der Grösse und der Komplexität ab. Dabei sind mehr oder weniger Risikoeigner:innen und Risikoverantwortliche aus den Bereichen im ICT-Risikomanagement-Prozess eingebunden. Unter dieser Annahme ergibt sich ein Gesamtaufwand von drei bis fünf Arbeitstagen pro Bereich im Zweijahresrhythmus.

Auf Wunsch der Bereiche oder bei grösseren Änderungen an IT-Systemen sowie bei der Einführung neuer wichtiger Fachanwendungen kann die Periodizität verkürzt werden.

Durch die Umsetzung risikomindernder Massnahmen können in den einzelnen Bereichen zusätzliche Aufwände oder Kosten entstehen. Diese werden im Rahmen des ordentlichen Budgetprozesses berücksichtigt.

8. Fazit

Mit dem stadtweiten ICT-Risikomanagement entsteht eine einheitliche, systematische Grundlage für den Umgang mit ICT-Risiken. Die Bereiche werden zentral durch die ICT Risikomanager:in unterstützt, bleiben jedoch für die Umsetzung verantwortlich. So ergibt sich eine konsolidierte Sicht auf die ICT-Risiken pro Bereich und Departement. Risiken können frühzeitig erkannt, gezielt behandelt und wirksam reduziert werden – was die Resilienz der Stadtverwaltung stärkt.

Zugleich lassen sich Kosten im Störfall senken, Investitionen optimieren und die Dienstleistungsqualität steigern. Das ICT-Risikomanagement unterstützt die Einhaltung gesetzlicher Vorgaben und fördert die kontinuierliche Verbesserung.

9. Zeitlicher Ablauf

Der Rollout des stadtweiten ICT-Risikomanagements ist wie folgt geplant:

Tätigkeiten	Zeitpunkt
Finalisierung aller Vorbereitungsaufgaben zum ICT-Risikomanagement	Bis Ende 2025
Start Rollout ICT-Risikomanagement mit 2-3 Bereichen (Pilotphase)	Q1 2026
Konsolidierung der Resultate aus Pilotphase	Q2 2026
Start Rollout ICT-Risikomanagement in allen Bereichen der Stadtverwaltung	Ab Q3 2026

10. Externe und interne Kommunikation

Es ist keine Medienmitteilung vorgesehen. Die Mitarbeitenden der Stadtverwaltung werden intern über den Beschluss informiert.

Beilage:

1. Konzept «Stadtweites ICT-Risikomanagement»