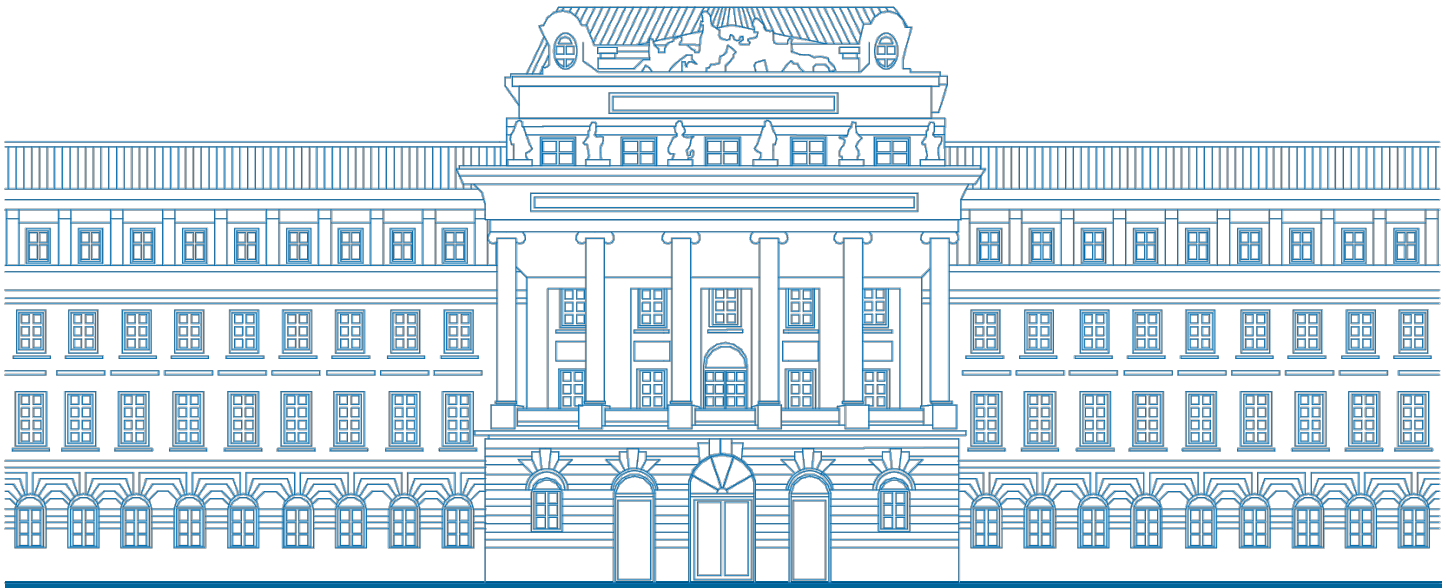
TECHNISCHE UNIVERSITÄT WIEN

RM Richtlinie

Richtlinie zum Risikomanagement



(online 14.12.2022)

Verlautbarung im Mitteilungsblatt Nr. 50/2022 vom 15.12.2022 (lfd. Nr. 523)

Dokumenteninformation

Beschluss des Rektorats am	13.12.2022
Sachbearbeiter_innen	Mag. Jörg Ponier
GZ:	6300.00/034/2022
Fassung vom:	13.12.2022

INHALT

PRÄAMBEL 4

1 EINLEITUNG 5

1.1 Corporate Governance 5
1.1.1 Compliance 6
1.1.2 Internes Kontrollsystem (IKS) 6
1.1.3 Risikomanagement 7
1.1.4 Interne Revision 7

1.2 Anwendungsbereich und Zielsetzung 8

1.3 Risikomanagement Prinzipien 9

1.4 Risikogruppen 10
1.4.1 Universitäre Umfeldrisken 10
1.4.2 Risikogruppe Compliance und Meldeverstöße 10
1.4.3 Risikogruppe Finanzen 10
1.4.4 Risikogruppe Forschung und Drittmittel 10
1.4.5 Risikogruppe Gebäude und Infrastruktur 10
1.4.6 Risikogruppe Personal 10
1.4.7 Risikogruppe Studium und Lehre 10

1.5 Rollen des Risikomanagements 11
1.5.1 Aufbauorganisation 11
1.5.2 Rektorat 12
1.5.3 Risikogruppenverantwortliche_r 12
1.5.4 Risikoverantwortliche_r 12
1.5.5 RM Beauftragte_r 13

2 RISIKOMANAGEMENTPROZESS 14

2.1 Risikoidentifikation 14

2.2 Risikobewertung 14
2.2.1 Eintrittswahrscheinlichkeit 14
2.2.2 Schadenshöhe 14
2.2.3 Risikovorsorge 14
2.2.4 Monitoring Risiken 15

2.3 Risikosteuerung 15
2.3.1 Risikovermeidung 15
2.3.2 Risikoreduktion 15
2.3.3 Risikoabwälzung 16
2.3.4 Risikoakzeptanz 16

2.4 Jährlicher RM-Kreislauf 16

2.5 Unterjähriger Meldeprozess 17

2.6 Berichterstattung 20
2.6.1 Jährliche Berichterstattung von dem_der RM Beauftragten 20
2.6.2 Kommunikation mit der Abteilung Interne Revision (E014) 20

2.7 Dokumentation und Ablage 20
2.7.1 Richtlinie 20
2.7.2 Risikokatalog 20

3 INKRAFTTRETEN 21

4 ANHANG 22

Präambel

Die Technische Universität Wien (TU Wien) steht für die Entwicklung wissenschaftlicher Exzellenz und die Vermittlung umfassender Kompetenz.

Mit der Umsetzung des Public Corporate Governance Kodex (B-PCGK) [1], gewährleistet die TU Wien, die Einhaltung der folgenden Punkte:

- Gemäß 9.1.4.1 B-PCGK sorgt die Geschäftsleitung für ein angemessenes Risikomanagement und -controlling.
- Gemäß 11.1.1.2. B-PCGK ist der Universitätsrat für die Überwachung des Risikomanagements verantwortlich.

Aus dem §22 Abs 1. Zi.17 UG 2002 ergibt sich ebenfalls die Verpflichtung für:

- „Die Errichtung eines Planungs- und Berichterstattungssystems, das die Erfüllung der Berichterstattungspflichten durch die Universitäten nach den gesetzlichen Vorschriften und den Vorgaben der Bundesministerin oder des Bundesministers für Finanzen hinsichtlich der Einrichtung eines Beteiligungs- und Finanzcontrolling gewährleistet.“ [2]

Detaillierter werden die Vorgaben des §22 Abs 1. Zi.17 UG 2002 im §2 Abs. 1 Beteiligungs- und Finanzcontrolling-Verordnung geregelt.

- „Das Beteiligungscontrolling umfasst die betriebswirtschaftliche Berichterstattung über monetäre und nicht-monetäre Kennzahlen auf Basis von Soll-Ist-Vergleichen sowie das Risikocontrolling im Wege der Berichterstattung über Risikoidentifikation und -bewertung.“ [3]

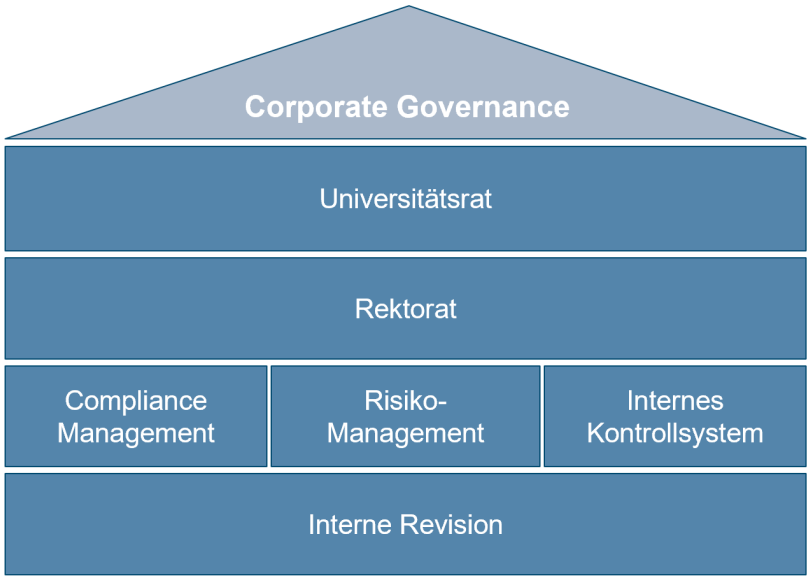
Die TU Wien betreibt bereits seit einigen Jahren ein Risikomanagement (kurz „**RM**“). Mit dieser Richtlinie wird nun ein einheitlicher Umgang mit Risiken an der TU Wien definiert.

[1] Public Corporate Governance Kodex (B-PCGK)
[2] Universitätsgesetz 2002
[3] Beteiligungs- und Finanzcontrolling Verordnung

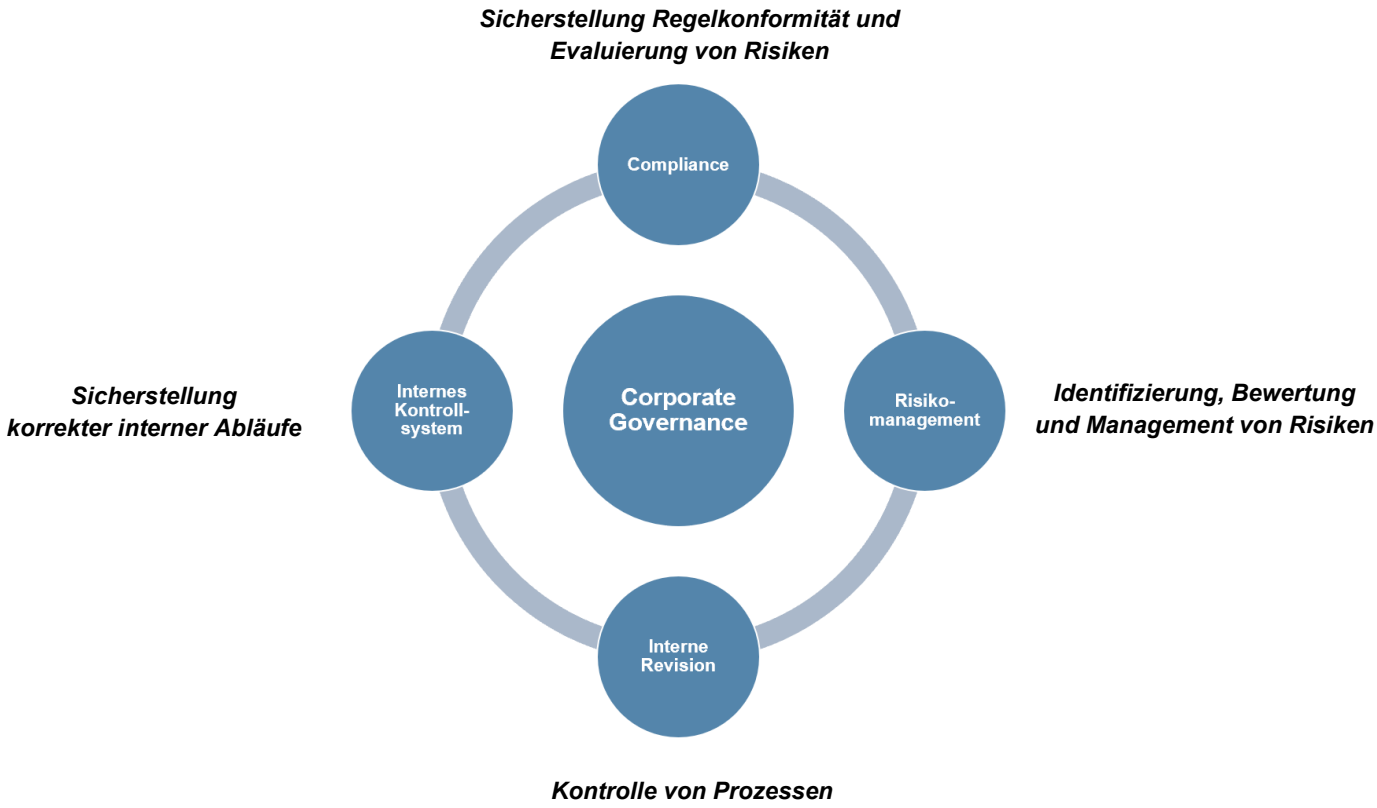
1 Einleitung

1.1 Corporate Governance

Corporate Governance bezeichnet alle internen Regeln, Prozesse und Gesetze (Unternehmensverfassung), nach denen ein Unternehmen geführt oder betrieben wird. Demnach handelt es sich bei der Corporate Governance der TU Wien um den faktischen und rechtlichen Ordnungsrahmen für die Leitung und Überwachung der Universität.



Zu den wesentlichen Instrumenten der Corporate Governance gehören das Risiko- und das Compliance-Management-System, das interne Kontrollsystem (IKS) und schließlich die Interne Revision. Die entsprechenden Instrumente verbessern die Führungs- und Überwachungsstrukturen der TU Wien und zielen auf die Sicherstellung einer nachhaltigen Entwicklung der TU Wien ab.



1.1.1 Compliance

Compliance umfasst einerseits die Einhaltung von universitätsinternen Regelungen (wie Satzungsteile, Verordnungen, Richtlinien, und Policies) sowie von (Geschäfts-)Prozessen (Sicherstellung Regelkonformität) sowie andererseits die Evaluierung von möglichen Risikofeldern (Evaluierung von Risiken) zur Verhinderung von Rechtsverstößen. Das Compliance Management System ist der Prozess, der es erlaubt, spezifische Risiken strukturiert zu identifizieren, darauf zu reagieren, diese zu mitigieren und in weiterer Folge zu steuern und zu überwachen.[4]

1.1.2 Internes Kontrollsystem (IKS)

Das IKS hat seinen Fokus auf rein finanzrelevante Risiken, die durch die Durchführung der Key Controls im Zuge operativer Tätigkeiten minimiert bzw. eliminiert werden sollen. Die Ausrichtung des IKS ist deshalb prozessorientiert, wobei eine der zentralen Aufgaben, die Sicherstellung korrekter interner Abläufe darstellt.

[4] Siehe Compliance Policy

Compliance	Internes Kontrollsystem
Vermeidung von Risiken (insbesondere zivilrechtliche und strafrechtliche Konsequenzen) für Organisation und Verantwortungsträger infolge von Nicht-Einhaltung von Normen.	Gewährleistung des Erreichens der Organisations-/Unternehmensziele durch Minimierung der Risiken der Organisation
Die Konzepte betrachten die Maßnahmen (Festlegung von Verantwortlichkeiten und Prozessen), die in einer Organisation eingerichtet sind, um Regelkonformität sicherzustellen.	
Die Konzepte setzen sich mit der systematischen Gestaltung von Prozessen und Kontrollschritten auseinander.	

Quelle: Positionspaper des Rechnungshofs „Leitfaden zur Überprüfung von Internen Kontrollsystemen“ 2016/03.

1.1.3 Risikomanagement

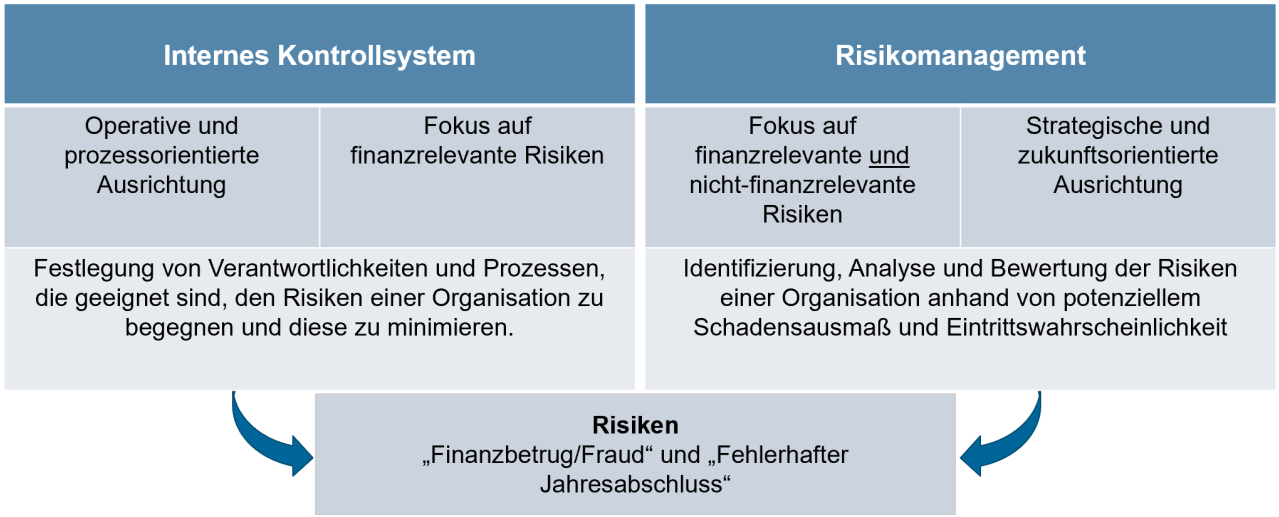
Unter einem Risikomanagement-System wird die Gesamtheit der Grundsätze, Verfahren und vorgegebenen Maßnahmen verstanden, die einen strukturieren Umgang mit Risiken – unabhängig ob finanzrelevante oder nicht-finanzrelevante Risiken – managt. Das Risikomanagement nimmt eine strategische und zukunftsorientierte Ausrichtung ein. Das Risikomanagement gliedert sich in die Teilbereiche (i) Identifizierung von Risiken (Risikoanalyse), (ii) Risikobewertung (Risikobeurteilung), (iii) Risikosteuerung und (iv) Risikocontrolling.

Unmittelbare Verbindungsglieder zwischen Risikomanagement und internes Kontrollsystem bilden inkludieren die beiden finanzrelevanten Risiken, „Finanzbetrug/Fraud“ und „Fehlerhafter Jahresabschluss“. Die Aufgabe des IKS besteht darin, die möglichen negativen Auswirkungen dieser beiden Risiken durch aufgesetzte Prozesse und definierte Key Controls zu minimieren bzw. im Idealfall auszuschließen.

1.1.4 Interne Revision

Die Aufgabe der Internen Revision besteht darin, interne Arbeitsprozesse auf deren Richtigkeit, Ordnungsmäßigkeit, Zweckmäßigkeit und Wirtschaftlichkeit zu prüfen und zu überwachen. Das Kontrollziel ist die Effizienzsteigerung und Risikominimierung und das Aufzeigen von Optimierungsbedarf gegenüber dem Rektorat und dem Universitätsrat.[5]

[5] Siehe Revisionsordnung



1.2 Anwendungsbereich und Zielsetzung

Der sachliche Anwendungsbereich des Risikomanagements umfasst sämtliche Bereiche (nämlich Zentraler Bereich und Fakultätsbereich) mit Risikopotenzial.

Zweck eines RM ist es,

- bestehende Risiken frühzeitig zu erkennen,
- zu bewerten und zu steuern
- um mit ausreichender Gewähr sicherstellen zu können,
- dass die betroffene Organisation im Rahmen der Erfüllung ihrer Aufgabenstellung ihre Ziele erreicht.

Verantwortlich für die operative Umsetzung des Risikomanagements sind die Mitarbeiter_innen, die einen Umgang mit Risiken pflegen müssen. Dabei zählen die Meldung und Bewertung von Risiken zu den zentralen Aufgaben von Leiter_innen. Commitment und Vorbildwirkung des Rektorats sind grundlegend für die Einrichtung, Aufrechterhaltung sowie die kontinuierliche Weiterentwicklung eines erfolgreichen RM („*tone at the top*“).

Grundlegende Risikoeinstellung der TU Wien

Die TU Wien verfolgt eine risikoaverse Risikoeinstellung, die in allen Handlungen der Mitarbeiter_innen ihre Berücksichtigung findet. Im Zuge der Risikosteuerung muss für jedes Risiko der optimale Umgang definiert werden.

Ziele des RM

- die Erreichung der Organisationsziele aus den Leitbildern der TU Wien „Technik für Menschen“ „Wissenschaftliche Exzellenz entwickeln“, „umfassende Kompetenz vermitteln“,
- Sicherung des Fortbestandes der Universität

Mit diesen Zielsetzungen werden nicht nur Chancen wahrgenommen, sondern auch Risiken eingegangen. Das primäre Ziel des Risikomanagements besteht darin, die Zielerreichung der TU Wien durch ein risikoaverses Agieren zu unterstützen.

1.3 Risikomanagement Prinzipien

- **Dokumentationsprinzip**
    - Klare, detaillierte und transparente Regelung des Umgangs mit definierten Risiken in schriftlicher Form.
    - Grundsatz der Nachvollziehbarkeit: Unterlagen sind nachvollziehbar zu dokumentieren.
- **Frühzeitige Risikoidentifizierung**
    - Schaffung von Risikobewusstsein bei Leiter_innen und Mitarbeiter_innen.
- **Realitätsnahe Risikobewertung**
    - Risikobewertung durch realistische Einschätzung aller relevanter Rahmenbedingungen auf Basis definierter Qualitätsstandards.
- **Optimale Risikosteuerung**
    - Der_die Risikoverantwortliche sollte, falls die Möglichkeit besteht, Maßnahmen zur Risikominimierung definieren können und den richtigen Umgang mit dem Risiko wählen.
    - Übernahme von Risikoverantwortung.
- **Unmittelbare Informationsweitergabe bei Risikoeintritt**
    - Ein unterjähriger Risikoeintritt eines Monitoring Risikos[6] ist unmittelbar an das Rektorat zu melden.
- **Regelmäßigkeit**
    - Regelmäßige und systematische Überprüfung des RM auf seine Funktionsfähigkeit, Wirksamkeit und Aktualität.
    - Sicherstellung, dass die genannten Gegenmaßnahmen dauerhaft und nachhaltig wirksam sind.
    - Jährlicher RM-Kreislauf mit jährlichen Aktualisierungen der bestehenden Risiken und Überprüfung der Bereiche auf Vollständigkeit der Risiken und in weiterer Folge Identifizierung und Bewertung von Risiken.
    - Bei Änderung der Rahmenbedingungen sind die Risiken | Gegenmaßnahmen entsprechend anzupassen → Zeitnahe Kontaktaufnahme mit RM-Beauftragte_n um Aktualisierung durchzuführen.
- **Wirtschaftlichkeit – Grundsatz der Kosten-Nutzen-Abwägung – Finanzintegrität**
    - Der mit Kontrollen verbundene Aufwand und Ressourceneinsatz muss in einem angemessenen Verhältnis zum vermeidbaren Risiko (Schadensausmaß und Eintrittswahrscheinlichkeit) stehen.

[6] Siehe 2.2.4 Monitoring Risiken

1.4 Risikogruppen

Die Risiken werden in Risikogruppen (RG) zusammengefasst und gegebenenfalls noch weiter untergliedert:

1.4.1 Universitäre Umfeldrisken

Diese Risikogruppe umfasst übergeordnete Risiken die in weiterer Folge alle Risikogruppen bereffen könnten. (Stand 2022: z.B.: Reaktorunfall, Pandemie, Naturkatastrophen, etc.).

1.4.2 Risikogruppe Compliance und Meldeverstöße

Diese Risikogruppe umfasst alle Risiken die im Zusammenhang mit Compliance und Meldeverstößen stehen.

1.4.3 Risikogruppe Finanzen

Die Risikogruppe Finanzen umfasst alle Risiken die ihren Ursprung in einem Finanzthema haben.
(Stand 2022: z.B.: Inflation, Unzureichende Finanzdeckung aufgrund niedrigen Abschlusses der Leistungsvereinbarung)

1.4.4 Risikogruppe Forschung und Drittmittel

Alle Risiken die mit der Durchführung von Forschung und Drittmittelprojekten zusammenhängen, werden hier aufgelistet.
(Stand 2022: z.B.: Scheitern eines großen Förderprojektes)

1.4.5 Risikogruppe Gebäude und Infrastruktur

Unter der Risikogruppe Gebäude- und IT Infrastruktur werden alle Risiken die im laufenden Betrieb auftreten können zusammengefasst. (Stand 2022: z.B.: Brände, Hackerangriffe)

1.4.6 Risikogruppe Personal

Hier werden alle Risiken erfasst, die im Bereich Personal vorkommen können.
(Stand 2022: z.B.: Berufungsabwehren, Kettenregeln)

1.4.7 Risikogruppe Studium und Lehre

Bei der Risikogruppe Studium und Lehre geht es primär um jene Risiken die mit der Durchführung von Lehre auftreten können. (Stand 2022: z.B.: Schlechtes Betreuungsverhältnis)

1.5 Rollen des Risikomanagements

1.5.1 Aufbauorganisation

Die RM-Aufbauorganisation besteht aus 3 Ebenen.

1. Ebene Rektorat

- Zweite (oberste) Meldestufe für einen tatsächlichen Risikoeintritt.
- Zweite (oberste) Eskalationsstufe bei Meldungsverzögerungen[7] der zu aktualisierenden Risiken.

2. Ebene Risikogruppenverantwortliche

- Erste Meldestufe für einen tatsächlichen Risikoeintritt.
- Erste Eskalationsstufe bei Meldungsverzögerungen der zu aktualisierenden Risiken.
- Zweite (oberste) Freigabestufe für aktualisierte und neu aufgenommene Risiken.

3. Ebene Risikoverantwortliche

- Risikoverantwortliche bilden die operative Ebene.
- Risikoverantwortliche müssen einen tatsächlichen Risikoeintritt an den_die Risikogruppenverantwortliche_n melden.
- Erste Freigabestufe für aktualisierte und neu aufgenommene Risiken.

[7] Siehe RM Workflow im Anhang

1.5.2 Rektorat

Die Aufgaben des Rektorats im Zusammenhang mit dem RM umfassen:

- Gesamtverantwortung für das RM in Bezug auf Umsetzung, Rollenverteilung, Aufrechterhaltung, Reporting
- Einbeziehung sämtlicher Bereiche der TU Wien in das RM.
- Festlegung der Ziele des RM in Abstimmung mit den Zielen der TU Wien.
- Die regelmäßige Beurteilung der Wirksamkeit des RM sowie die Überwachung der Umsetzungen von Verbesserung und notwendiger Maßnahmen.
- Bereitstellung von adäquaten Ressourcen zur Sicherstellung der Funktionsfähigkeit des RM.
- Commitment und Vorbildwirkung bei der Einhaltung der RM-Richtlinie („tone at the top“).
- Zweite (oberste) Meldestufe für einen tatsächlichen Risikoeintritt.
- Zweite (oberste) Eskalationsstufe bei Meldungsverzögerungen[8] der zu aktualisierenden Risiken.

1.5.3 Risikogruppenverantwortliche_r

- Risikogruppenverantwortliche sind die Mitglieder des Rektorats, der_die Leiter_in für Finanzen.
- Die Aufteilung der Risikogruppen erfolgt gemäß Geschäftsordnung des Rektorats. Die Risiken der Abteilung Finanzen werden dem_der Leiter_in für Finanzen zugeordnet.
- Die Rolle der Risikogruppenverantwortlichen ist nicht übertragbar.

Zum Verantwortungsbereich der Risikogruppenverantwortlichen gehört Folgendes:

- Ernennung von Risikoverantwortliche_n (nur eine Person pro Risiko).
- Erste Meldestufe für einen tatsächlichen Risikoeintritt.
- Ein tatsächlicher Eintritt eines Monitoring Risikos ist unmittelbar an das Rektorat und der_die RM Beauftragte_n zu melden.
- Die Weiterleitung eines tatsächlichen Eintritts eines Nicht-Monitoring Risikos liegt im Ermessen des_der Risikogruppenverantwortliche_n.
- Zweite (oberste) Freigabestufe für aktualisierte und neu aufgenommene Risiken.
- Unterjährig aufgenommene „Monitoring Risiken“[9] sind umgehend durch den_die Risikogruppenverantwortliche_n an das Rektorat und den RM Beauftragte_n zu kommunizieren.
- Erste Eskalationsstufe bei Meldungsverzögerungen von zu aktualisierenden Risiken.

1.5.4 Risikoverantwortliche_r

- Die Ernennung von Risikoverantwortlichen erfolgt durch den zuständigen Risikogruppenverantwortlichen.
- Zum Risikoverantwortlichen können nur Leiter_innen iSd Struktur und Governance der TU Wien[10] ernannt werden.
- Die Rolle der Risikoverantwortlichen ist nicht übertragbar, aber das Risikomanagement ist an Mitarbeiter_innen delegierbar.
- Im Anlassfall ist die Rolle der Risikoverantwortlichen vom zuständigen Risikogruppenverantwortlichen abzuerkennen.

Die Risikoverantwortlichen übernehmen die zentrale Rolle im RM. Zum Verantwortungsbereich der Risikoverantwortlichen gehört Folgendes:

- Verpflichtende Absolvierung der RM-Schulungen:
    - Allgemeine Schulung über Ziele, Prinzipien, Abläufe des RM und Abgrenzung zum Internen Kontrollsystem.
    - Spezielle Schulung zur Identifizierung von Risiken.
    - Spezielle Schulung zur Risikobewertung.

[8] Siehe RM Workflow im Anhang
[9] Siehe 2.2.4 Monitoring Risiken
[10] Siehe RL Struktur und Governance

- Verantwortung für die Vollständigkeit des RM in seinem_ihrem Bereich in Abstimmung mit dem_der zuständigen Risikogruppenverantwortlichen.
- Jährliche Prüfung bestehender Risiken auf Aktualität.
- Definition neuer Risiken und Meldung an Risikogruppenverantwortliche sowie an den RM Beauftragte_n (auch unterjährig - Die Freigabeschritte der jährlichen Aktualisierung kommen auch unterjährig zur Anwendung).
- Falls ein „Monitoring-Risiko“[11] eintritt (jährlich als auch unterjährig) ist dies durch den_die Risikoverantwortliche_n dem_r Risikogruppenverantwortlichen unmittelbar zu melden.
- Um die Aktualität der Bewertung der Risiken aufrecht zu erhalten, sorgen die Risikoverantwortlichen eigenständig für regelmäßige Prüfzyklen. Dadurch wird die Aufmerksamkeit für die Notwendigkeit der Risikomessung gewahrt, welche unterjährige Meldungen überhaupt erst möglich machen.
- Einhaltung definierter Qualitätsstandards bei Risikoidentifikation, -bewertung und -steuerung.
- Regelkonformes Agieren sowie die Einhaltung von Gesetzen und Richtlinien.
- Erste Freigabestufe für aktualisierte und neu aufgenommene Risiken.
- Einholung der Freigabe des Risikogruppenverantwortlichen für aktualisierte und neu aufgenommene Risiken.
- Ansprechpartner_in für den_die Risikogruppenverantwortliche_n, den_die RM Beauftragte_n und Interne Revision.
- Erstellung notwendiger begleitender Unterlagen.
- Kommunikation an alle von dem Risiko betroffene Mitarbeiter_innen.

1.5.5 RM Beauftragte_r

- Der_die RM Beauftragte_r wird vom gemäß Geschäftsordnung des Rektorats zuständigen Rektoratsmitglied bestellt.
- Direkte Unterstellung unter dem zuständigen Rektoratsmitglied.
- Die Rolle des RM Beauftragten kann nur vom zuständigen Rektoratsmitglied aberkannt werden.

Zu seinem_ ihrem Verantwortungsbereich zählt Folgendes:

- Koordination, Verwaltung, Dokumentation und Weitergabe der RM-Informationen an das Rektorat.
- Unterstützung und Hilfestellung bei Fragen zur Aufbau- und Ablauforganisation des RM.
- Empfehlungen an das Rektorat betreffend strategische und strukturelle Weiterentwicklung des RM.
- Initiierung von Maßnahmen zur Verbesserung des RM.
- Zentrale Verwaltung und Archivierung des Risikokatalogs.
- Hilfestellung bei der Aktualisierung von Risiken.
- Erstellung eines jährlichen RM-Berichts an das Rektorat (inklusive Meldung von Risiken in Zusammenhang mit der Umsetzung des RM).

[11] Siehe 2.2.4 Monitoring Risiken

2 Risikomanagementprozess

2.1 Risikoidentifikation

Risikoidentifikation ist die systematische Erfassung und Sammlung aller auf die TU Wien einwirkenden Risiken. Als Risikoidentifikation eignen sich verschiedene Instrumente wie beispielsweise Befragungen, Workshops, historische Entwicklungen, etc.

2.2 Risikobewertung

Die Risikobewertung erfolgt durch eine realistische Einschätzung von Schadenshöhe, Eintrittswahrscheinlichkeit und der bestehenden Risikovorsorge. Alle Risiken und Gegenmaßnahmen, die in einer Erhebung durch die Risikoverantwortlichen festgestellt wurden, werden im Risikokatalog aufgenommen. Für jedes Risiko sollte eine geeignete Gegenmaßnahme definiert werden. Ausnahmen müssen gesondert begründet werden.

Die Risikoklassifizierung der TU Wien sieht wie folgt aus:

2.2.1 Eintrittswahrscheinlichkeit

Score	Eintrittswahrscheinlichkeit
Score 1	sehr gering (letztes Risikoereignis liegt größer 10 Jahre zurück)
Score 2	gering (letztes Risikoereignis liegt zwischen 4 und 10 Jahren zurück)
Score 3	mittel (letztes Risikoereignis liegt zwischen 2 und 4 Jahren zurück)
Score 4	hoch (letztes Risikoereignis liegt maximal 2 Jahre zurück)

2.2.2 Schadenshöhe

Score	Schadenshöhe in (Mio.€)
Score 1	**unwesentlich < 0,3 pro Jahr** Keine spürbare Auswirkung auf Forschung oder Lehre
Score 2	**minimal 0,3 - 1 pro Jahr** Kleinere Beeinträchtigungen der Lehre und kleinere Behinderungen der Forschung
Score 3	**wesentlich 1 - 5 pro Jahr** Erhöhung des Dropouts und der Studiendauer sowie Verlust von Forschungskompetenz, -renommee (Drittmitteln)
Score 4	**gefährdend > 5 pro Jahr** Beinahe Zusammenbruch der Lehre, überwiegende Einstellung der Forschung

2.2.3 Risikovorsorge

In die Risikobewertung fließt auch ein, ob Maßnahmen zur Risikominimierung gesetzt wurden:

- Klar geregelte Verantwortung
- Vorhandener Maßnahmenkatalog
- Abgeschlossene Versicherung

Je nachdem wie viele Bedingungen erfüllt sind verändert sich der Score für die Risikobewertung.

Score	Strukturierter Umgang
Score 0	**Mindestens 2 Bedingungen sind erfüllt**
Score 1	**2 Bedingungen sind unklar bzw. nicht erfüllt**
Score 2	**3 Bedingungen sind unklar bzw. nicht erfüllt**

Die Risikobewertung wird damit abgeschlossen, indem die Summe aus den Scores für Eintrittswahrscheinlichkeit, Schadenshöhe und Risikovorsorge gebildet wird. Je nach Höhe der Summe erfolgt dann die Reihung der Risiken.

2.2.4 Monitoring Risiken

Ergibt die Risikobewertung eine Summe der Scores von mindestens 5 und weist eine Schadenshöhe von größer 2 auf, so zählt dieses Risiko zur Gruppe der Monitoring Risiken. Diese Risiken können bestandsgefährdend sein, daher stehen sie unter laufender Beobachtung durch den_die Risikoverantwortliche_n und sind Teil des jährlichen Risikoberichts des_der Risikomanagementbeauftragten ans Rektorat.

Falls ein Monitoring-Risiko eintreten könnte tt ist dies durch den_die Risikoverantwortliche_n unmittelbar dem_r Risikogruppenverantwortlichen zu melden, der dies wiederum umgehend an das Rektorat und den_die Risikomanagementbeauftragte_n zu melden hat.

2.3 Risikosteuerung

Die Risikosteuerung definiert die verschiedenen Ansätze im Umgang mit Risiken. Unterschieden werden 4 Ansätze die je nach Risiko zur Anwendung kommen können:

- Risikovermeidung
- Risikoreduktion
- Risikoabwälzung
- Risikoakzeptanz

2.3.1 Risikovermeidung

Bei der Risikovermeidung geht es darum, den Eintritt von Risiken auszuschließen. Daher versteht man darunter die Beendigung bereits geplanter unternehmerischer Aktivitäten um den Risikoeintritt zu verhindern. Diese weitreichende Entscheidung kommt nur dann zur Anwendung, wenn es keine geeigneten Maßnahmen bzw. nur unzureichende Maßnahmen gibt um das Risiko angemessen zu reduzieren.

2.3.2 Risikoreduktion

Unter Risikoreduktion versteht man die Verminderung von Risikoquellen und damit in weiterer Folge die Reduzierung der Eintrittswahrscheinlichkeit und/oder des Schadensausmaßes. Das lässt sich oftmals mit Richtlinien, klar definierten Prozessen, technischen Hilfsmitteln (Systeme, etc.) sowie Schulungen realisieren.

2.3.3 Risikoabwälzung

Risiken können auch auf Dritte wie beispielweise Versicherungen, Lieferanten, Projektpartner etc. übertragen werden. Bedingt dadurch, dass diese Abwälzung des Risikos meistens an eine finanzielle Gegenleistung gekoppelt ist, muss eine Kosten-Nutzen-Abwägung getroffen werden. Im Einzelfall kann auch das in Kaufnehmen eines Schadenereignisses günstiger sein als die Abwälzung des Risikos.

2.3.4 Risikoakzeptanz

Die letzte verbleibende Möglichkeit im Umgang mit Risiken ist die Akzeptanz. Manche Risiken werden billigend in Kauf genommen um Chancen nützen zu können. Der Hauptfokus liegt darin, den Fortbestand der TU Wien nicht zu gefährden. In der Regel handelt sich dabei um Risiken mit einer geringen Eintrittswahrscheinlichkeit und einem geringen Schadensausmaß. Dieser Kategorie sind auch jene Risiken zuzuordnen an dessen Eintritt man selbst mit Gegenmaßnahmen nichts ändern kann, wie beispielsweise einer Pandemie.

2.4 Jährlicher RM-Kreislauf

Der jährliche RM Kreislauf zeigt den Workflow des Risikomanagements der jedes Jahr zu durchlaufen ist:

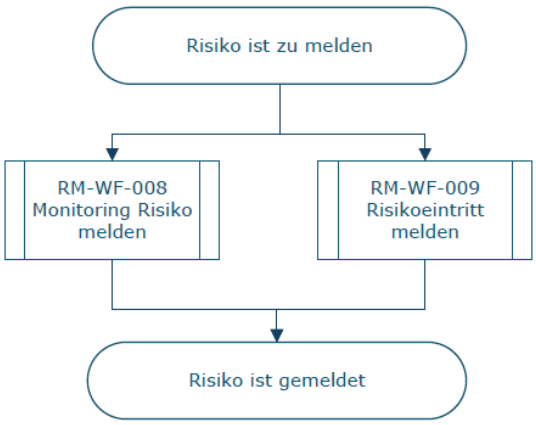
Legende
RGV … Risikogruppenverantwortliche_r
RV … Risikoverantwortliche_r
RK … Rektorat

Die mit dieser Richtlinie freigegebenen RM-Workflow (siehe Anhang) erläutern den jährlichen RM-Kreislauf detailliert.

2.5 Unterjähriger Meldeprozess

RM-WF-007 Risiko melden (unterjährig)

Input	Ablauf	Output	D	E	M	I



RM-WF-008 Neues Monitoring Risiko melden

Input	Ablauf	Output	D	E	M	I
	Neues Monitoring Risiko ist zu melden					
	Risiko entwickelt sich bei unterjähriger Risikobewertung zu Monitoring Risiko		RV	-	-	-
	Meldung an den Risikogruppenverantwortliche_n		RV	-	-	RGV
	Rektorat und RM Beauftragte_n über „Monitoring Risiko" informieren		RGV	-	-	RK RMB
	Neues Monitoring Risiko ist gemeldet					

Legende

D ... Durchführung
E ... Entscheidung
M ... Mitarbeit
I ... Information

KC ... Key Control

RGV ... Risikogruppenverantwortliche_r
RK ... Rektorat
RMB... RM Beauftragte_r
RV ... Risikoverantwortliche_r

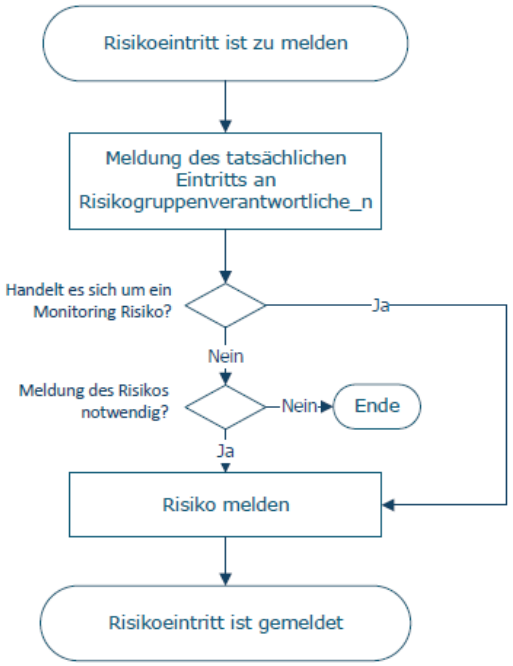
Prozessinformation

Aufgezeichnet:	E. Schmid-Müllegger
Prozessverantwortliche_r:	P. Ponier
Freigegeben:	M. Kolassa

Version:	v0
Datum:	2022-12-05

RM-WF-009 Risikoeintritt melden

Input	Ablauf	Output	D	E	M	I
	Risikoeintritt ist zu melden					
	Meldung des tatsächlichen Eintritts an Risikogruppenverantwortliche_n		RV	-	-	RGV
	Handelt es sich um ein Monitoring Risiko?		-	RGV	-	-
	Meldung des Risikos notwendig?		-	RGV	-	-
	Risiko melden		RGV	-	-	RK RMB
	Risikoeintritt ist gemeldet					



Legende

D ... Durchführung
E ... Entscheidung
M ... Mitarbeit
I ... Information

KC ... Key Control

RGV ... Risikogruppenverantwortliche_r
RK ... Rektorat
RMB... RM Beauftragte_r
RV ... Risikoverantwortliche_r

Prozessinformation

Aufgezeichnet:	E. Schmid-Müllegger
Prozessverantwortliche_r:	P. Ponier
Freigegeben:	M. Kolassa
Version:	v0
Datum:	2022-12-05

2.6 Berichterstattung

2.6.1 Jährliche Berichterstattung von dem_der RM Beauftragten

Der_die RM Beauftragte berichtet zumindest einmal jährlich dem Rektorat:

- RM Konzept (Rückblick und Ausblick)
- Risikoevaluierung
- Kosten des RM im Vorjahr
- Sonstige Themen
- Risikokatalog

2.6.2 Kommunikation mit der Abteilung Interne Revision (E014)

Der_die RM Beauftragte ist Ansprechperson für die Prüfungen der Abteilung Interne Revision (E014).

2.7 Dokumentation und Ablage

2.7.1 Richtlinie

Die RM Richtlinie ist auf der Website von E018 Datenschutz und Dokumentenmanagement für alle Mitarbeiter_innen der TU Wien (Login erforderlich) abrufbar.

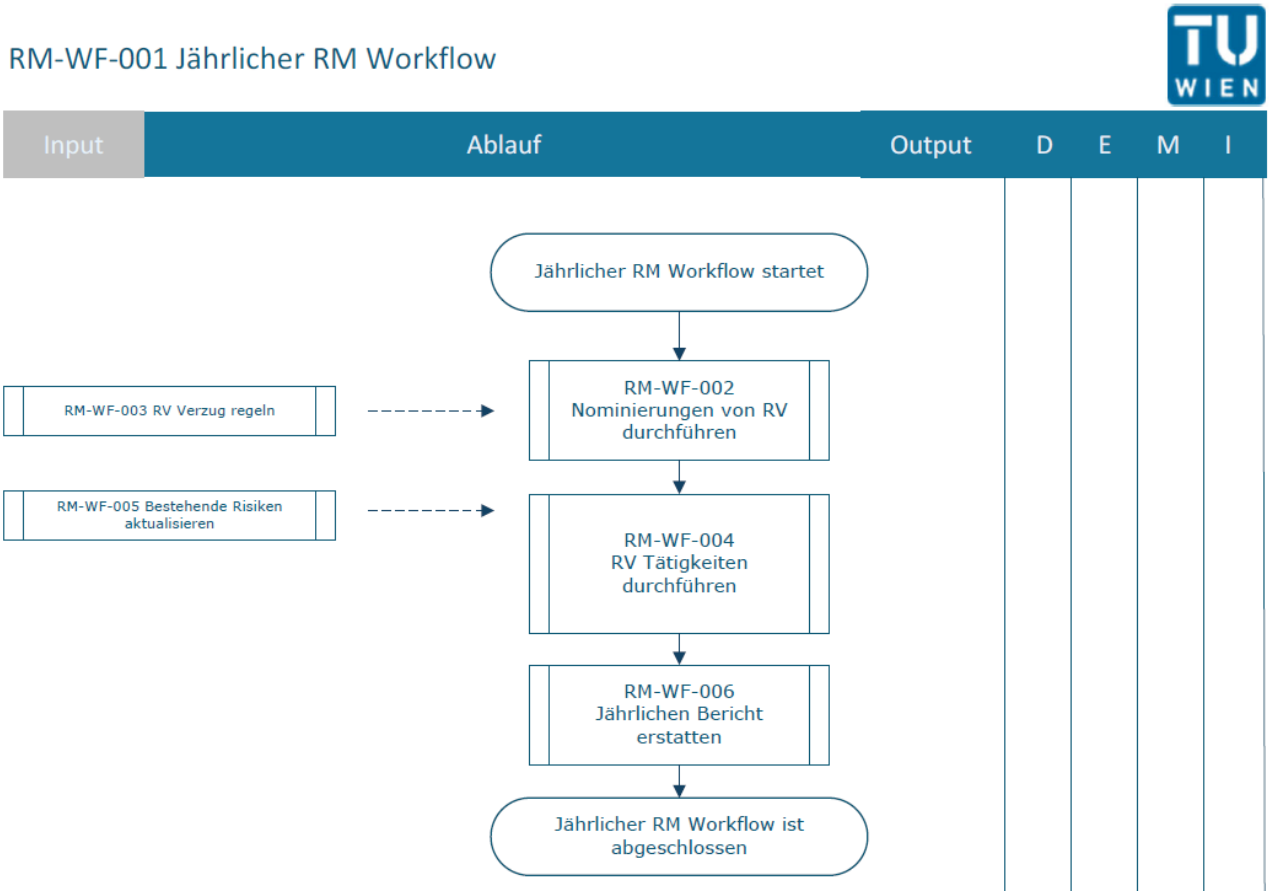
2.7.2 Risikokatalog

Alle identifizierten und bewerteten Risiken sind im Risikokatalog aufgelistet, dieser wird auf der Website des_der RM-Beauftragte_e für alle Mitarbeiter_innen der TU Wien (Login erforderlich) zugänglich gemacht..

3 Inkrafttreten

Die RM-Richtlinie wird vom Rektorat beschlossen und tritt am Tag der Veröffentlichung im Mitteilungsblatt in Kraft.

4 Anhang


RM-WF-001 Jährlicher RM Workflow
Input
Ablauf
Output
D
E
M
I
Jährlicher RM Workflow startet
RM-WF-003 RV Verzug regeln
RM-WF-002 Nominierungen von RV durchführen
RM-WF-005 Bestehende Risiken aktualisieren
RM-WF-004 RV Tätigkeiten durchführen
RM-WF-006 Jährlichen Bericht erstatten
Jährlicher RM Workflow ist abgeschlossen

Legende

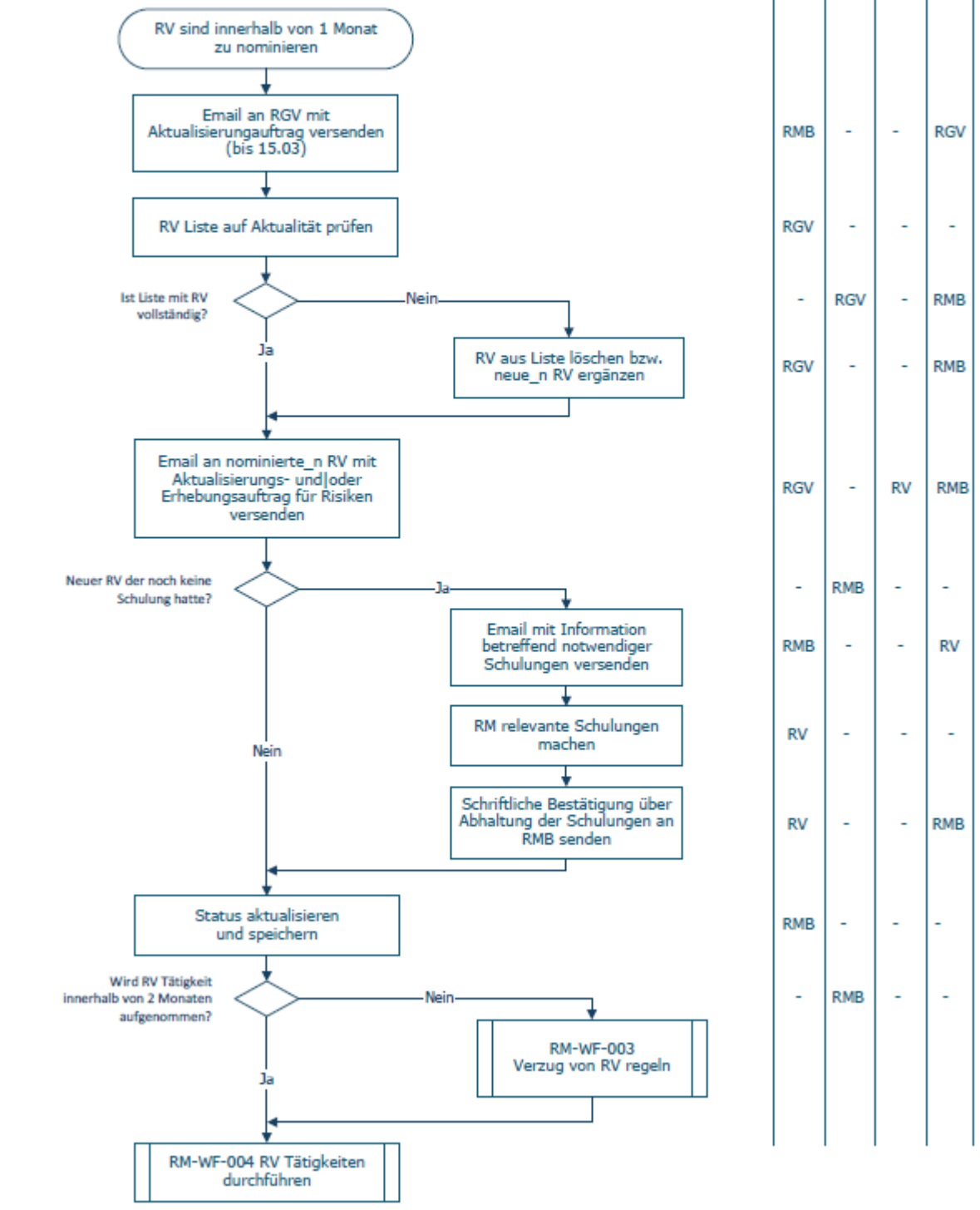
D ... Durchführung
E ... Entscheidung
M ... Mitarbeit
I ... Information

KC ... Key Control

Prozessinformation

Aufgezeichnet:	E. Schmid-Müllegger
Prozessverantwortliche_r:	P. Ponier
Freigegeben:	M. Kolassa
Version:	v0
Datum:	2022-11-03

RM-WF-002 Nominierungen von RV durchführen



Legende

D ... Durchführung
E ... Entscheidung
M ... Mitarbeit
I ... Information

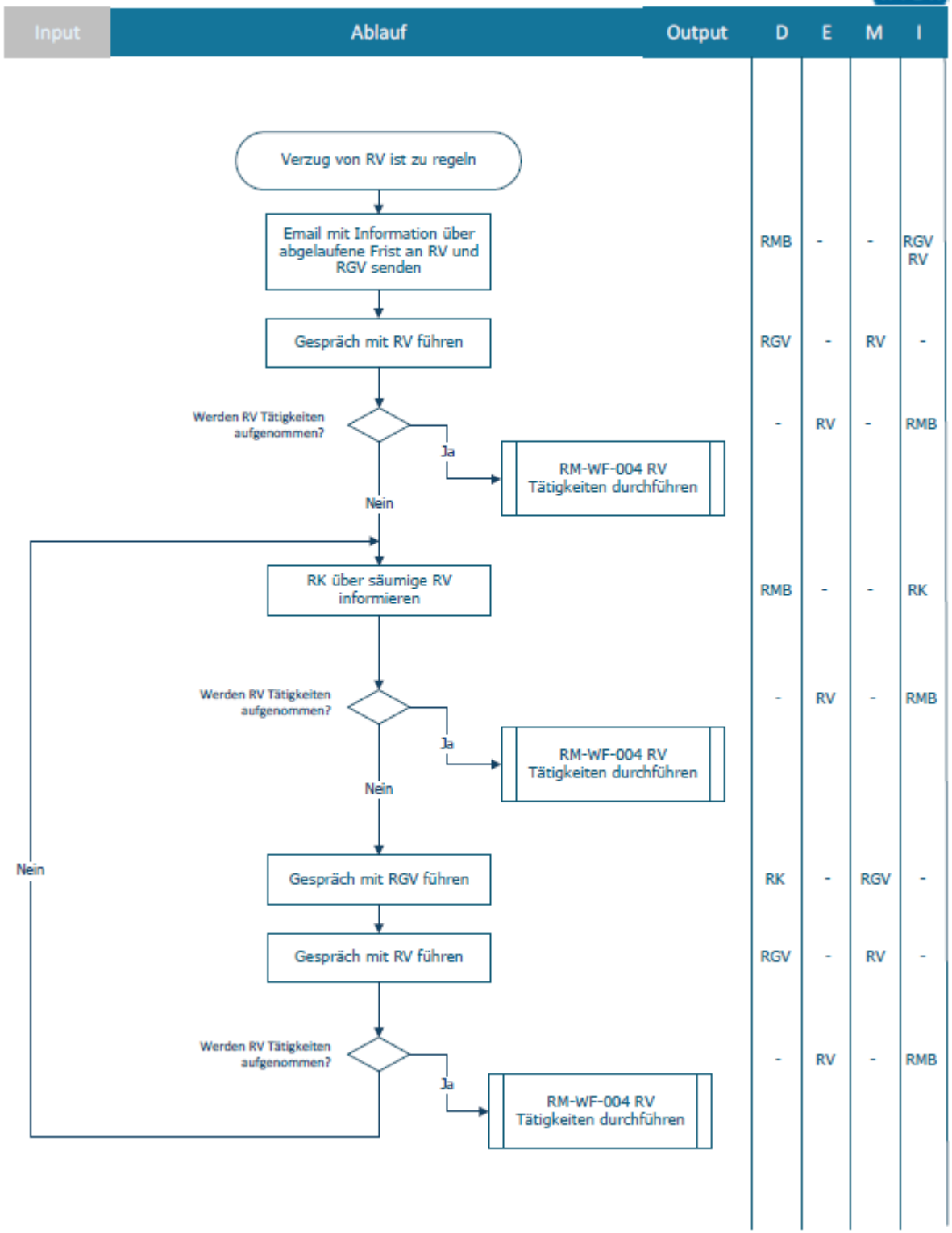
KC ... Key Control

RMB... RM Beauftragte_r
RGV ... Risikogruppenverantwortliche_r
RV ... Risikoverantwortliche_r

Prozessinformation

Aufgezeichnet:	E. Schmid-Müllegger
Prozessverantwortliche_r:	P. Ponier
Freigegeben:	M. Kolassa
Version:	v0
Datum:	2022-11-03

RM-WF-003 Verzug von RV regeln



Legende

D ... Durchführung
E ... Entscheidung
M ... Mitarbeit
I ... Information

KC ... Key Control

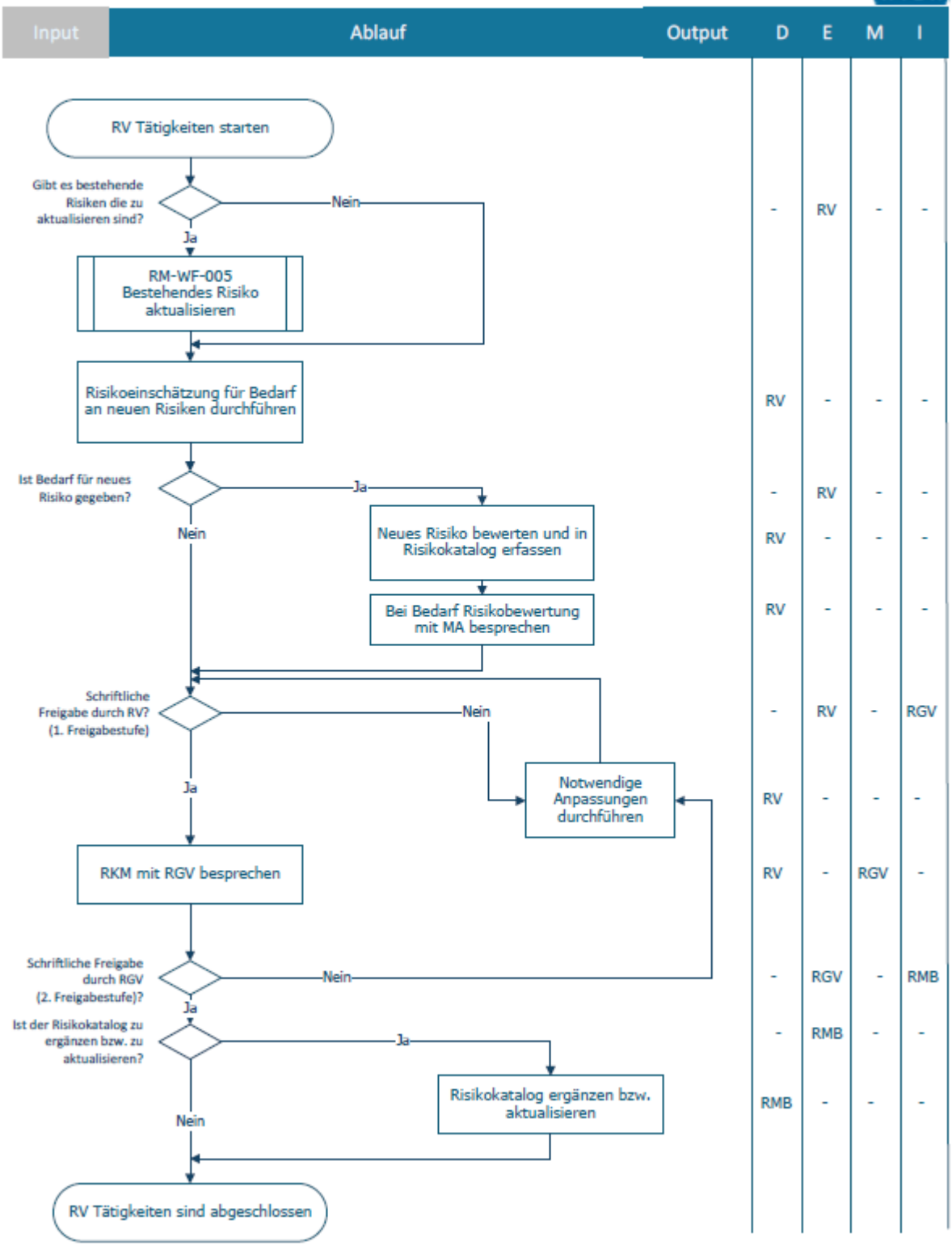
RMB... RM Beauftragte_r
RGV ... Risikogruppenverantwortliche_r
RV ... Risikoverantwortliche_r
RK ... Rektorat

Prozessinformation

Aufgezeichnet:	E. Schmid-Müllegger
Prozessverantwortliche_r:	P. Ponier
Freigegeben:	M. Kolassa

Version:	v0
Datum:	2022-11-03

RM-WF-004 RV Tätigkeiten durchführen



Legende

D ... Durchführung
E ... Entscheidung
M ... Mitarbeit
I ... Information

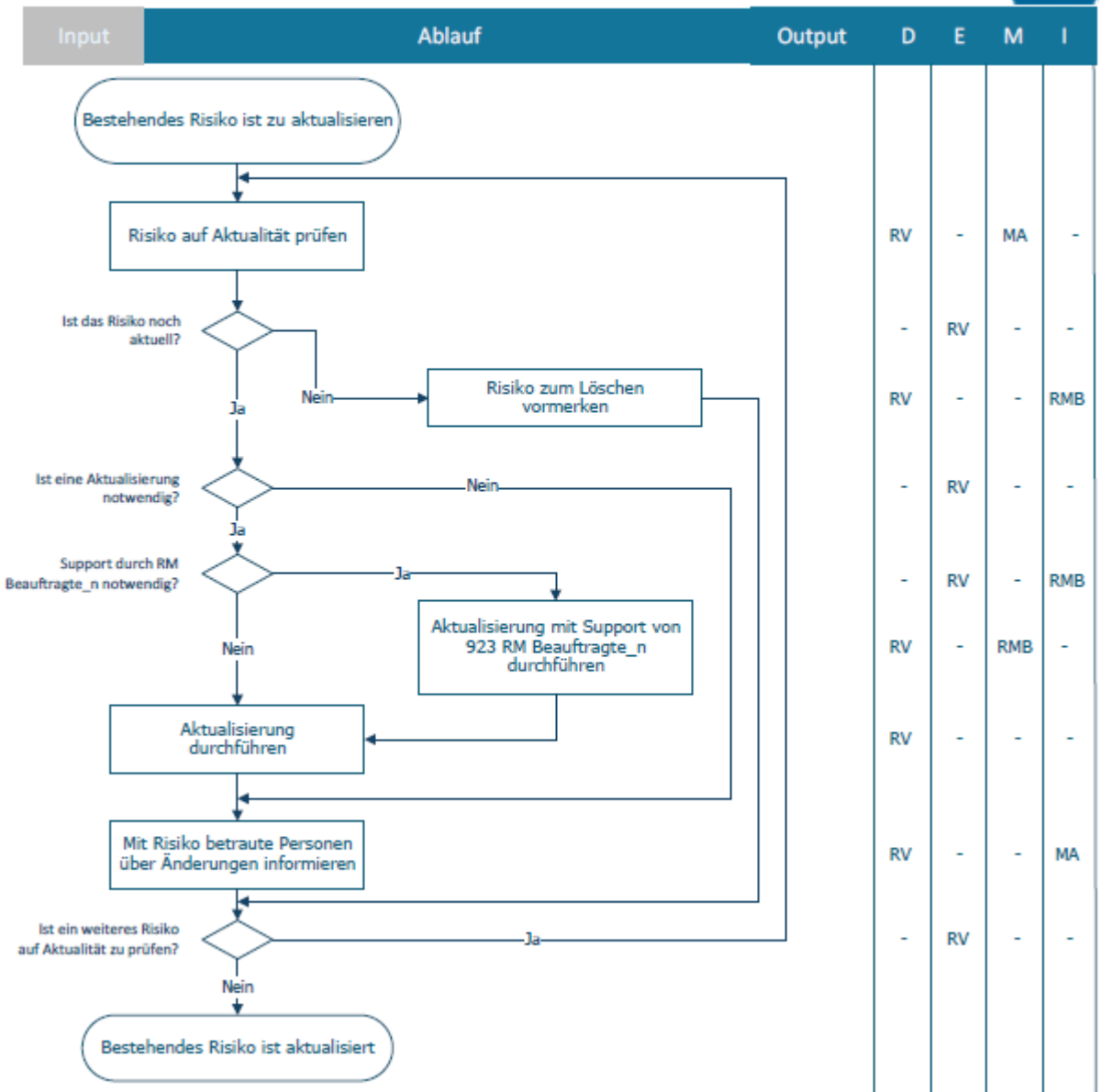
KC ... Key Control

RMB... RM Beauftragte_r
RGV ... Risikogruppenverantwortliche_r
RV ... Risikoverantwortliche_r

Prozessinformation

Aufgezeichnet:	E. Schmid-Müllegger
Prozessverantwortliche_r:	P. Ponier
Freigegeben:	M. Kolassa
Version:	v0
Datum:	2022-11-22

RM-WF-005 Bestehendes Risiko aktualisieren



Legende

D ... Durchführung
E ... Entscheidung
M ... Mitarbeit
I ... Information

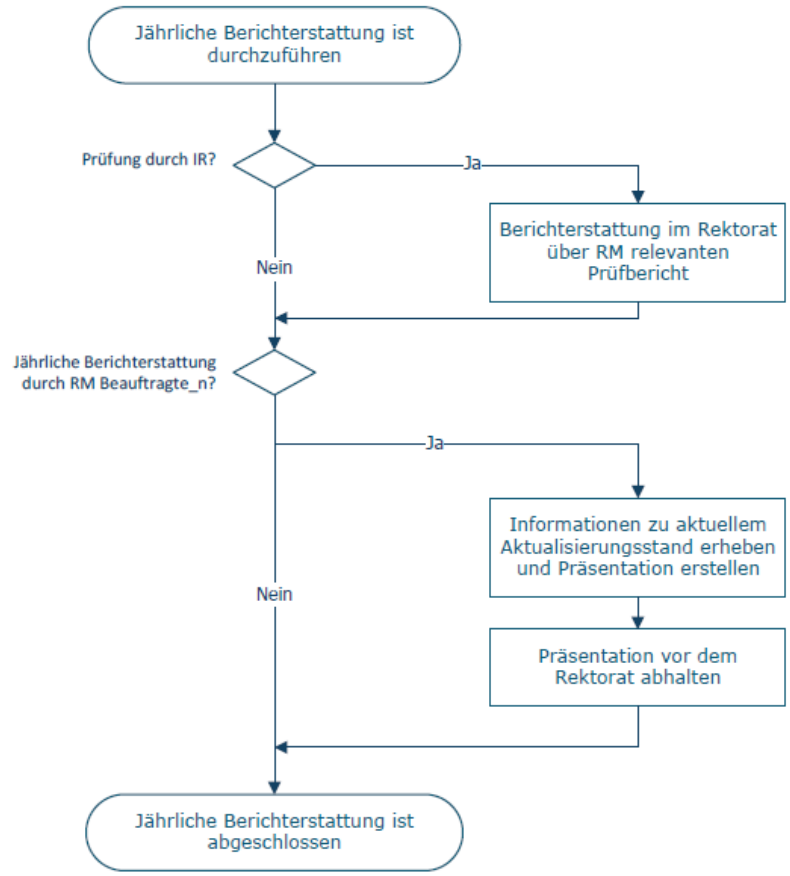
KC ... Key Control

RMB... RM Beauftragte_r
MA ... Mitarbeiter_in
RV ... Prozessverantwortliche_r

Prozessinformation

Aufgezeichnet:	E. Schmid-Müllegger
Prozessverantwortliche_r:	P. Ponier
Freigegeben:	M. Kolassa
Version:	v0
Datum:	2022-11-03

RM-WF-006 Jährlichen Bericht erstatten



Input	Ablauf	Output	D	E	M	I
	Prüfung durch IR?	-	-	IR	-	-
	Berichterstattung im Rektorat über RM relevanten Prüfbericht	IR	IR	-	RK	-
	Jährliche Berichterstattung durch RM Beauftragte_n?	-	-	RMB	-	-
	Informationen zu aktuellem Aktualisierungsstand erheben und Präsentation erstellen	RMB	RMB	-	-	-
	Präsentation vor dem Rektorat abhalten	RMB	RMB	-	RK	-

Legende

D … Durchführung
E … Entscheidung
M … Mitarbeit
I … Information

KC … Key Control

RMB… RM Beauftragte_r
IR… Interne Revision
RK … Rektorat

Prozessinformation

Aufgezeichnet:	E. Schmid-Müllegger
Prozessverantwortliche_r:	P. Ponier
Freigegeben:	M. Kolassa
Version:	v0
Datum:	2022-11-03