Richtlinie zum Internen Kontrollsystem (IKS)

RL 96000 IKSY 131-02

Technische Universität Graz
Rechbauerstraße 12
A-8010 Graz
Telefon +43 (0) 316 873 / 0

	Erstellt	Geprüft	Freigegeben
Name	*Vizerektorat Personal und Finanzen*	*Rektorat*	*Rektoratsbeschluss*
Datum	*09.01.2020*	*21.01.2020*	*21.01.2020*

INHALT

1. Zweck

Zweck dieser Richtlinie ist die Einhaltung der IKS-Prinzipien.

2. Geltungsbereich

Die IKS-Richtlinie gilt für alle Organisationseinheiten (OE) der TU Graz. Abweichungen bedürfen der Genehmigung des Rektorats.

Die Geltungsdauer ist unbefristet.

3. Verteiler

An alle Mitarbeiter/innen der TU Graz

4. Gegenseitige Beziehungen

Im Falle des Nichteinhaltens von Vorschriften durch eine OE der TU Graz haftet diese OE dem Rektorat im Innenverhältnis für alle dadurch verursachten Schäden.

5. Mitgeltende Unterlagen

Universitätsgesetz 2002 (UG) BGBI I 2002/120 idgF

Satzung und Richtlinien der TU Graz in der geltenden Fassung

6. Prozessverantwortlichkeit

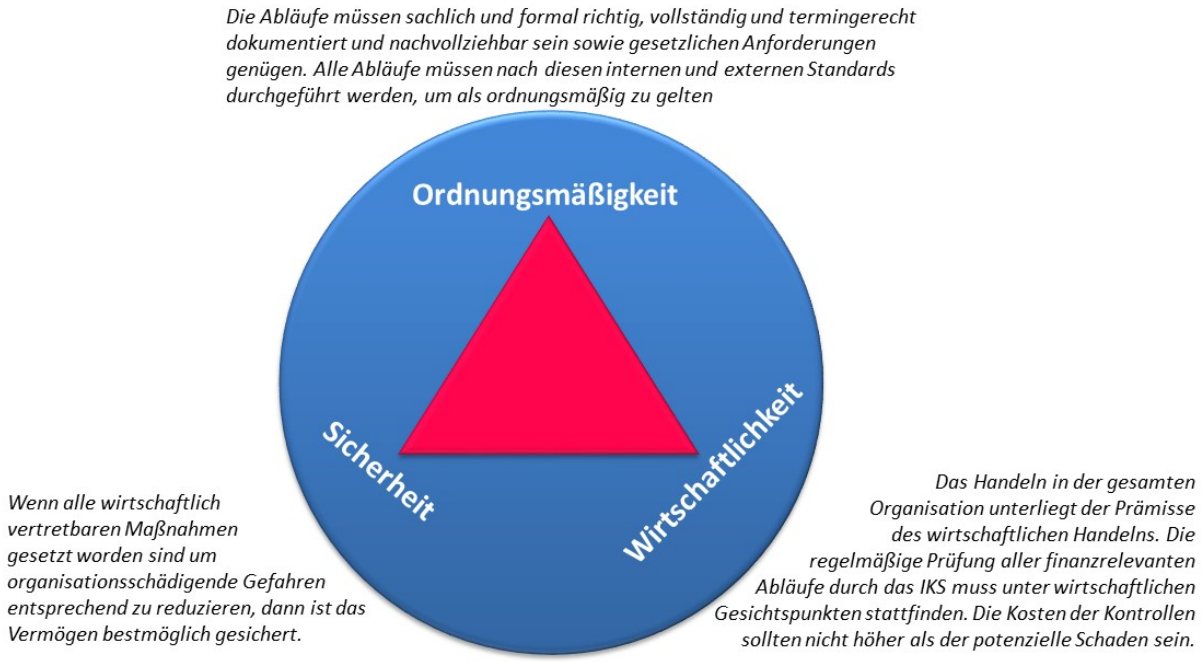
Rektorat

7. Internes Kontrollsystem

7.1. Allgemeines

7.1.1. Definition des Internen Kontrollsystems

Unter einem Internen Kontrollsystem (IKS) ist die Gesamtheit aller prozessbezogenen Methoden und Maßnahmen zu verstehen, die an der TU Graz dazu dienen, die Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit der internen Abläufe zu gewährleisten.



Die interne Kontrolle ist ein in die Arbeits- und Betriebsabläufe einer Organisation eingebetteter Prozess, der von den Führungskräften und den Mitarbeiterinnen und Mitarbeitern durchgeführt wird, um

- bestehende Risiken zu erfassen,
- zu steuern und

- mit ausreichender Gewähr sicherstellen zu können, dass die betreffende Organisation im Rahmen der Erfüllung ihrer Aufgabenstellung ihre Ziele erreicht.

Sicherzustellende Ziele sind:

- Sicherung der Vermögenswerte vor Verlust, Missbrauch und Schaden,
- Erreichung der Organisationsziele,
- Sicherstellung ordnungsgemäßer, ethischer, wirtschaftlicher, effizienter und wirksamer Abläufe,
- Zuverlässigkeit von betrieblichen Informationen; insbesondere Zuverlässigkeit des Rechnungswesens,
- die Einhaltung der Gesetze und Vorschriften,
- die Erfüllung der Rechenschaftspflicht („accountability“ / „answerability“)

7.1.2. Begriffsabgrenzungen

IKS und Risikomanagement sind untrennbar miteinander verbunden. Das IKS soll sicherstellen, dass das Erreichen der Organisationsziele nicht durch interne und externe Risiken gefährdet wird. Zur Beurteilung der Qualität eines IKS ist die Kenntnis der Risiken der Organisation bzw. der Abläufe unabdingbar. Das Risikomanagement ist damit Grundvoraussetzung und Basis des IKS.
Interne Kontrollsysteme müssen bei Änderungen der Risikosituation angepasst werden.

7.1.3. Angewandte Standards

Der Ablauf des Risikomanagementprozesses orientiert sich hierbei am internationalen Standard - ISO 31000 Risikomanagement Grundsätze – Richtlinie. Es handelt sich dabei um einen wiederkehrenden Prozess zur Sicherstellung einer strukturierten Vorgehensweise unter Berücksichtigung aller relevanten Informationen.
Das Interne Kontrollsystem ist angelehnt an das Vorgehensmodell des COSO Modell für Interne Kontrollsysteme (Committee of Sponsoring Organizations), welches ebenfalls einen international anerkannten Standard darstellt.

Die Interne Revision arbeitet grundsätzlich nach den „Internationalen Standards für die berufliche Praxis der Internen Revision 2017 (IPPF – The International Professional Practice Framework)“.

7.1.4. IKS Prinzipien

Das IKS an der TU Graz umfasst Maßnahmen und Kontrollen, mit denen das vorhandene Vermögen geschützt und gesichert wird und dadurch die fristgerechte und ordnungsmäßige Erstellung des Rechnungsabschlusses gewährleistet wird:

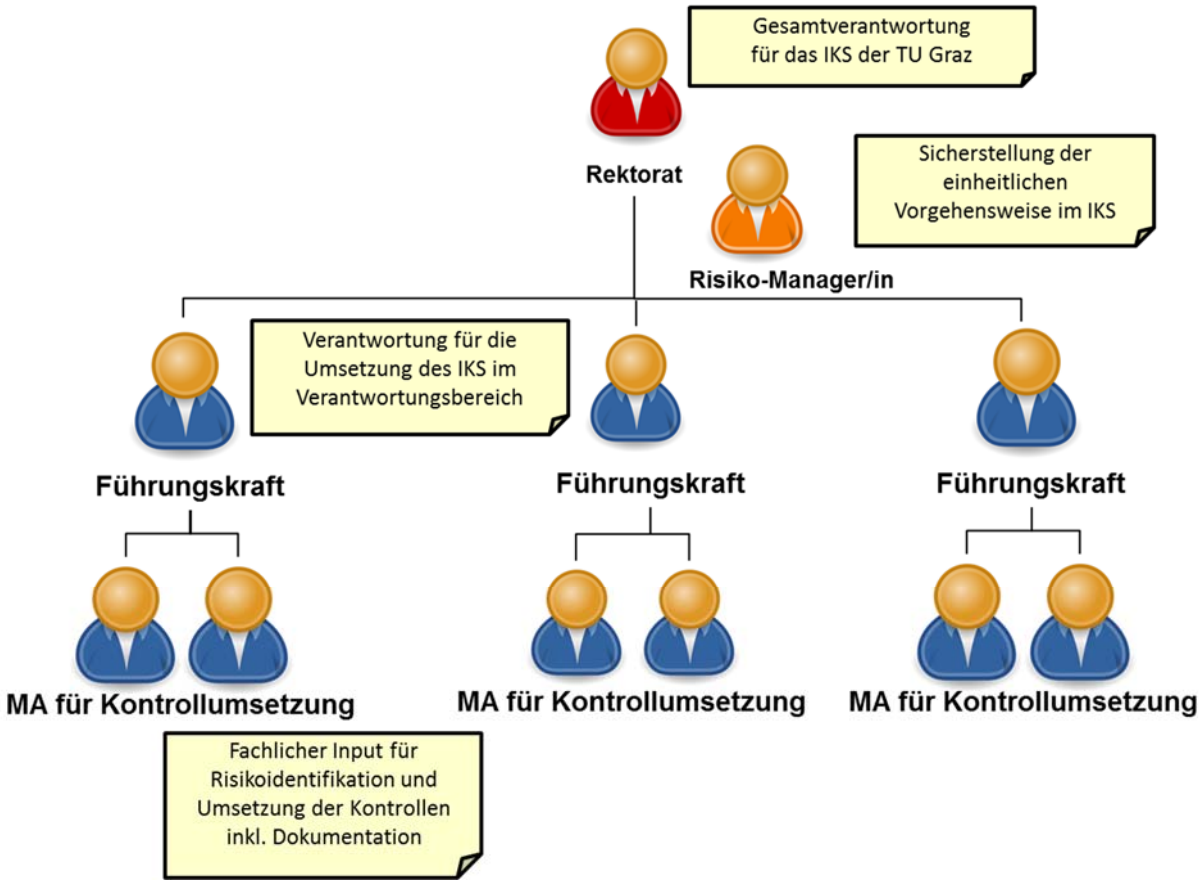
- Transparenz-Prinzip: klare, detaillierte und transparente Regelung der Arbeitsabläufe in schriftlicher Form. Unterlagen und Abläufe sind nachvollziehbar zu dokumentieren.
- Kontrollautomatik und Mehr-Personen-Prinzip: systematischer Einbau von Kontrollen im Arbeitsablauf (Kontrollautomatik), z.B. IT-gestützt (automatisierte Systemkontrollen) oder durch Implementierung des Vier-Augen-Prinzips.
- Prinzip der Funktionstrennung: keine Allein-Verantwortung für den gesamten Prozess. Konsequente Trennung von entscheidender, ausführender und kontrollierender Funktion.
- Aufgaben- und verantwortungsadäquate Informationsbereitstellung (Prinzip der Mindestinformation): Bereitstellung jener Information an Management und Mitarbeiter/innen, die zur Erfüllung der Aufgaben notwendig sind.
- Aufgaben- und verantwortungsadäquate Zugangs- und Zugriffsberechtigungen (Prinzip der „minimalen Rechte“): Zugangs- und Zugriffsberechtigungen (z.B. zu IT-Systemen) müssen adäquat beschränkt sein. Einräumung nur jener Berechtigungen zu sensiblen Daten, die zur Erfüllung der Aufgaben unbedingt erforderlich sind.
- IKS als rollierender Prozess: regelmäßige und systematische Überprüfung des IKS auf seine Funktionsfähigkeit, Wirksamkeit und Aktualität, um sicherzustellen, dass die internen Kontrollen dauerhaft/nachhaltig wirksam sind und bei Änderung der Rahmenbedingungen entsprechend angepasst werden.

- Grundsatz der Kosten-Nutzen-Abwägung: der mit Kontrollen verbundene Aufwand/Ressourceneinsatz muss in einem angemessenen Verhältnis zum zu vermeidenden Risiko (Schadenshöhe und Eintrittswahrscheinlichkeit) stehen.

7.1.5. Mindestanforderungen an das Interne Kontrollsystems

- Die Festlegung von Zielen und Festlegungen zur grundsätzlichen strategischen Ausrichtung der Organisation durch die Leitungsebene
- Prozessbeschreibungen bzw. Richtlinien, die für die Hauptprozesse standardisierte Abläufe und klare Verantwortungen definieren
- Verfügbarkeit relevanter Informationen als Grundlage für die Organisationssteuerung und damit auch für ein adäquates IKS
- Risikoanalysen als Entscheidungsgrundlage für die Maßnahmen zur Risikominimierung bzw. Festlegung von Kontrollen
- Die Dokumentation der Kontrollen, um das Handeln nachvollziehbar und überprüfbar zu machen

7.2. Verantwortlichkeiten



7.2.1. Rektorat

Das Rektorat der TU Graz definiert die zu erfüllenden Vorgaben, dargestellt in der IKS-Richtlinie, für die Umsetzung, legt die Zielsetzungen und die Reportingstruktur fest. Das Rektorat trägt die Verantwortung für die Einrichtung, Aufrechterhaltung und kontinuierliche Weiterentwicklung des IKS an der TU Graz.

Die Interne Revision, die direkt dem/der Rektor/in unterstellt ist, überwacht durch systematische Prüfungen die Ordnungsmäßigkeit, Rechtmäßigkeit, Funktionsfähigkeit und Wirtschaftlichkeit der betrieblichen Abläufe sowie die Wirksamkeit des IKS.

7.2.2. Führungskraft

Die Führungskraft stellt die Zweckmäßigkeit der zugeordneten Arbeitsabläufe sicher. Sie verantwortet die (Teil-) Aufgaben vom Start bis zum Ende und zeichnet für die Zielerreichung, den Inhalt, die Ergebnisse und die Schnittstellen verantwortlich.
Die Führungskraft identifiziert Risiken und definiert im Ablauf die wesentlichen Kontrollen. Diese werden in die Risiko-Kontroll-Matrix übergeführt und periodisch überprüft. Damit ist die Führungskraft für die Minimierung der Risiken verantwortlich.

Rollenbeschreibung: Führungskraft im IKS	
Zweck der Rolle	▪ Aktive Risikosteuerung für die verantworteten Risiken ▪ Überwachung der Umsetzung der Kontrollmaßnahmen für die zugeordneten Risiken
Aufgaben/Pflichten/ Verantwortlichkeiten	▪ Identifikation und Bewertung der Risiken ▪ Festlegung von geeigneten Kontrollen und deren Verantwortung ▪ Laufende Überwachung der Rückmeldungen zur Kontrollumsetzung im Verantwortungsbereich ▪ Periodisches Review der Risiken sowie deren Dokumentation ▪ Wirksamkeitsprüfung der definierten Kontrollmaßnahmen ▪ Einleitung von Korrekturmaßnahmen bei Abweichungen von Kontrollergebnissen

7.2.3. Risiko Manager/in

Diese zentrale Stelle hat die Aufgabe, das Risikomanagement & Interne Kontroll-System der TU Graz als Steuerungs- und Überwachungsinstrument zur Verfügung zu stellen. Organisatorisch ist es die Leitung der Serviceeinrichtung Beteiligungs- und Risikomanagement.

Rollenbeschreibung: Risiko Manager/in	
Zweck der Rolle	▪ Aufbau und kontinuierliche Weiterentwicklung des Internen Kontrollsystems ▪ Festlegung und Anpassung von IKS-Grundlagen für die TU Graz
Aufgaben/Pflichten/ Verantwortlichkeiten	▪ Aufbau, kontinuierliche Verbesserung und Dokumentation des IKS

	▪ Schaffung und Sicherstellung der Einhaltung von organisationsweit geltenden IKS-Standards ▪ Aufbau und Betreiben des zentralen IKS-Reportings ▪ Methodische Unterstützung der Führungskräfte ▪ Übergeordnete Überwachung und Einforderung der Umsetzung des IKS ▪ Zentrale Ansprechstelle für die Führungskräfte der TU Graz in Bezug auf IKS
Abgrenzung/ Nicht-Ziel	▪ Festlegung der Risiken und Kontrollen (da dies von der jeweilig zugeordneten Führungskraft zu erfolgen hat) ▪ Wissen über alle Risiken und Kontrollen bis in tiefste Detailebene ▪ Verantwortlichkeit für die operative Durchführung von Kontrollen

7.3. Finanzrelevante Prozesse

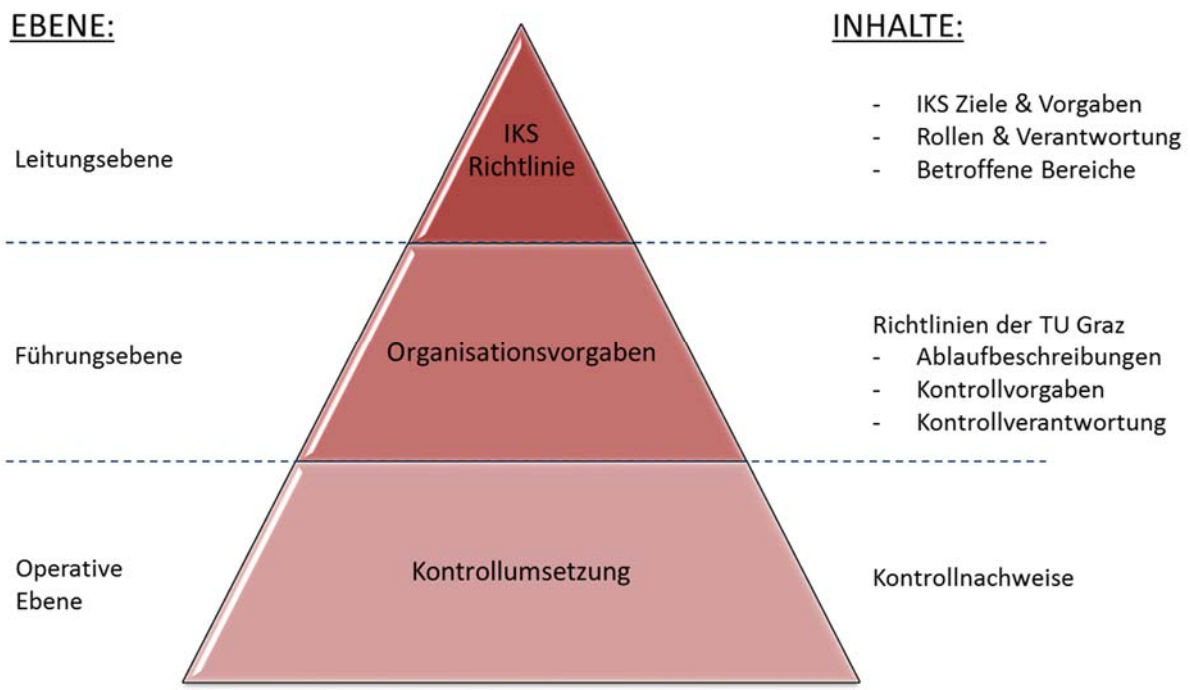
Die Beurteilung der Risiken erfolgt für die nachfolgend aufgeführten Prozesse:

- Beschaffung
- Finanzen
    - Budgetierung
    - Berichtswesen
    - Steuerung
    - Rechnungslegung
    - Veranlagung
- Drittmittel und Fundraising
- IT-Nutzung
- Personaladministration und Reisen
- Beteiligungen

7.4. IKS Dokumentation der Prozesse

Die Geschäftsprozesse und Arbeitsabläufe an der TU Graz werden laufend innerhalb von Richtlinien dokumentiert und stetig weiterentwickelt. Sie sind für die Mitarbeiter/innen im Intranet „TU4U“ einsehbar.

Die Risiken betreffend die Prozesse und Abläufe werden in einer Risiko-Kontrollmatrix festgehalten.



7.4.1. Risiko-& Kontrolldokumentation

Das Risikomanagement wird jährlich einer Evaluierung unterzogen und die Risiken sind in einem Risikokatalog erfasst. Dabei werden die Risiken jeweils von den OE-LeiterInnen im ersten Quartal zum Stand vom 31.12. des Vorjahres überprüft und ggf. neue Risiken gemeldet. Die Bewertung erfolgt anhand der unter 7.4.2 aufgeführten Kriterien.

Im Sinne des IKS sind weiters den Risiken aus den finanzrelevanten Prozessen entsprechend zweckmäßige Kontrollmaßnahmen zuzuordnen. Diese Kontrollen werden in einer Risiko-Kontrollmatrix dargestellt.

7.4.2. Risikobewertung

Schadenswahrscheinlichkeit		
Kategorie Einstufung	Eintrittswahrscheinlichkeit	Beschreibung
1	seltener als alle 25 Jahre	Das Risiko kann nicht ausgeschlossen werden; der Eintritt kann bei Einhaltung der dem Stand der Technik entsprechenden Vorbeugungsmaßnahmen und den vorgeschriebenen Kontrollen als unwahrscheinlich beurteilt werden.
2	Alle 5-25 Jahre	Das Risiko ist realistisch und im Universitätenvergleich bekannt; die vorliegenden Vorbeugungsmaßnahmen werden als geeignet zur Vermeidung beurteilt.
3	Alle 1-5 Jahre	Das Risiko muss als möglich angenommen werden; aus Universitätenvergleichen ist bekannt, dass sich derartige Schäden relativ häufig ergeben.
4	mehrmals jährlich	Das Risiko kann innerhalb des Zeitraums mehrmals auftreten; dies gehört zum normalen Geschäftsablauf (Frequenzschaden).

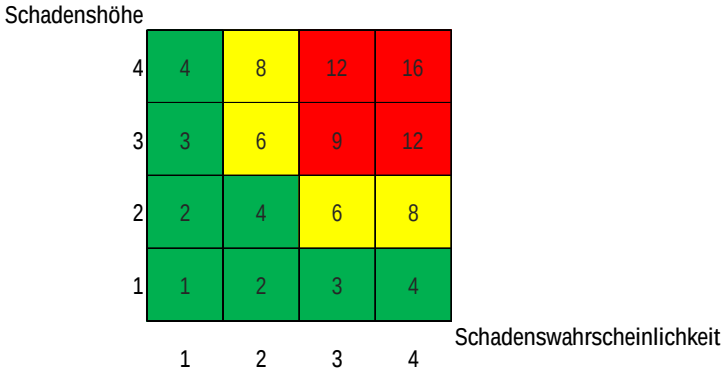
Schadenshöhe					
Kategorie Einstufung	monetär (bezogen auf ein Jahr)	Image	Image Beschreibung/Erläuterung	Gesundheit	Auswirkungen auf laufenden Universitätsbetrieb
1	<100 TEUR	interner Erklärungsbedarf	Die Reputation wird nach Außen kaum beeinträchtigt. Es entsteht intern Erklärungsbedarf.	Leichter Gesundheitsschaden mit vorübergehenden Beschwerden, Arbeitszeitausfall bis zu 3 Tagen	Beeinträchtigung einzelner Bereiche, stundenweise
2	> oder = 100 TEUR & <1.000 TEUR	regionale negative Berichterstattung	Es kommt zu Nachfragen von Außen die regionalen Medien interessieren sich für das Vorkommnis. Der externe Erklärungsbedarf hat noch keine direkten und anhaltenden Folgen.	Schwerer Gesundheitsschaden ohne Dauerfolgen, Arbeitszeitausfall mehr als 3 Tage (z.B. Knochenbruch)	kurzer Stillstand des Gesamt-Betriebes, < 1 Tag
3	> oder = 1.000 TEUR & < 10Mio	nationale negative mediale Aufmerksamkeit	Die Reputation der Universität wird durch negative Berichte und Medienberichterstattung (u.a. Social Media) beeinträchtigt. Angehende Studierende/potenzielle Mitarbeiterinnen und Mitarbeiter bevorzugen nach Möglichkeit andere Bildungseinrichtungen.	Schwerer Gesundheitsschaden mit Dauerfolgen / Tätigkeitseinschränkungen (z. B. Invalidität)	kurzer anhaltender Stillstand des Gesamt-Betriebes, ein Tag bis eine Woche
4	> oder = 10 Mio.	internationale negative Information. Mediale Aufmerksamkeit	Die Reputation wird überregional irreparabel geschädigt. Das Vertrauen in die Führung ist erschüttert, deshalb ist die Kapazitätsauslastung der Universität nicht mehr sichergestellt. Abwanderung von Schlüsselkräften	Personenschaden mit Todesfolge	länger anhaltender Stillstand des Gesamt-Betriebes, > eine Woche

7.4.3. Bewertungsmatrix

Maßnahme zur Reduktion des Risikos

Besondere Beobachtung
Halbjährig Aug. / Jan-Feb

Maßnahmen nicht zwingend notwendig
nächste Regelbewertung August



7.4.4. Risiko-Kontrollmatrix

Die Risiko-Kontrollmatrix stellt den Zusammenhang zwischen den identifizierten und bewerteten Risiken und den zweckmäßig zugeordneten Kontrollen dar. Dabei werden u.a. Kontrollaufgabe /-inhalt, Kontrollverantwortung und ggf. Nachweise dargestellt.

7.4.5. Ablage der IKS Dokumentation

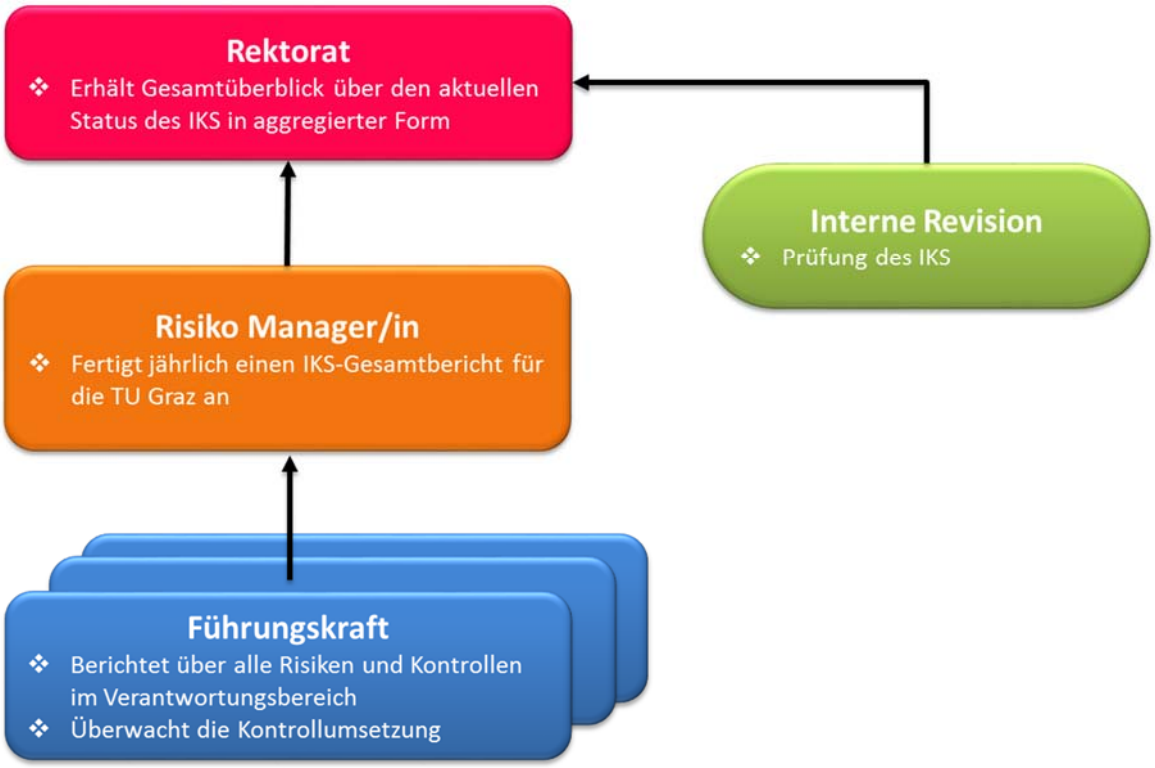
Alle Richtlinien befinden sich im Intranet der TU Graz „TU4U“ und sind allen Mitarbeiterinnen und Mitarbeitern zugänglich. Die Risiko-Kontrollmatrix ist Bestandteil des Risikokatalogs der TU Graz. Die Ablage und der Zugriff wird durch den/die Risiko Manager/in koordiniert.

7.4.6. Evaluierung der Kontrollen

Die Risiken werden regelmäßig auf ihre Aktualität überprüft und es werden entsprechende Kontrollen auf Vollständigkeit, Zweckmäßigkeit, Einhaltung und Wirksamkeit durchgeführt. Die Evaluierung der Kontrollen sowie deren Umsetzung und Dokumentation erfolgt durch die jeweilige Führungskraft.

7.5. Berichterstattung

Das Reporting betreffend IKS soll sicherstellen, dass die notwendigen Kontrollen definiert, umgesetzt und wirksam sind. Aus diesem Grund werden einerseits die Risiken und andererseits die Umsetzung der Kontrollen wiederkehrend in periodischen Abständen, zumindest jährlich berichtet.



Absender	Empfänger	Inhalte	Format	Zeitpunkt
Führungs-kräfte	Risiko Manager/in	Risikolage im Ver-antwortungsbereich Kontrollumsetzung	Aktualisierte Ver-sion des Risikoka-talogs & der Risiko-Kontroll-matrix	Ende 1. Quartal
Risiko Manager/in	Rektorat	Überblick zur Um-setzung des IKS Überblick zur aktuellen Risikolage	IKS-Gesamtbericht	Ende 2. Quartal
Führungs-kräfte	Risiko Ma-nager/in	Ad-hoc Risiken Kontrollabweichun-gen	E-Mail	Ad hoc