MITTEILUNGSBLATT

der

UNIVERSITÄT GRAZ

74. SONDERNUMMER

Studienjahr 2022/23 | Ausgegeben am 07. 06. 2023 | 33.a Stück

IKS-Handbuch

Beschluss des Rektorats vom 25.05.2023

Impressum: Medieninhaberin, Herausgeberin und Herstellerin: Universität Graz, Universitätsplatz 3, 8010 Graz. Verlags- und Herstellungsort: Graz.
Anschrift der Redaktion: Rechts- und Organisationsabteilung, Universitätsplatz 3, 8010 Graz.
E-Mail: mitteilungsblatt@uni-graz.at
Internet: https://mitteilungsblatt.uni-graz.at/

Offenlegung gem. § 25 MedienG
Medieninhaberin: Universität Graz, Universitätsplatz 3, 8010 Graz. Unternehmensgegenstand: Erfüllung der Ziele, leitenden Grundsätze und Aufgaben gem. §§ 1, 2 und 3 des Bundesgesetzes über die Organisation der Universitäten und ihre Studien (Universitätsgesetz 2002 - UG), BGBl. I Nr. 120/2002, in der jeweils geltenden Fassung.
Art und Höhe der Beteiligung: Eigentum 100%.
Sitz: Universitätsplatz 3, 8010 Graz
Namen der vertretungsbefugten Organe des Medieninhabers: Dr. Peter Riedler, Univ.-Prof. Dr. Joachim Reidl, Univ.-Prof. Dr. Catherine Walter-Laager, Univ.-Prof. Dr. Markus Fallenböck, LL.M., Univ.-Prof. Mireille van Poppel, PhD
Grundlegende Richtung: Kundmachung von Informationen gem. § 20 Abs. 6 UG in der jeweils geltenden Fassung.

UNIVERSITÄT GRAZ
UNIVERSITY OF GRAZ

IKS-Handbuch

Inhalt

Abkürzungsverzeichnis

AG IKS	Arbeitsgruppe Internes Kontrollsystem
BMBWF	Bundesministerium für Bildung, Wissenschaft und Forschung
B-PCGK 2017	Bundes Public Corporate Governance Kodex 2017
COSO	Committee of Sponsoring Organizations of the Treadway Commission
Einheiten	Fakultäten und akademische Einheiten, Verwaltungseinheiten, universitäts- und fakultätsübergreifende Leistungsbereiche
IKS	Internes Kontrollsystem
RKM	Risikokontrollmatrix
UG	Universitätsgesetz 2002
Uni Graz	Universität Graz

1 Präambel

Die Universität Graz (i. F. kurz Uni Graz) ist eine Forschungsinstitution des 21. Jahrhunderts, für die vor mehr als 430 Jahren der Grundstein gelegt wurde. Wir sehen es als unsere Aufgabe an, uns mit zentralen gesellschaftlichen Themen auseinanderzusetzen, Problemlösungen aufzuzeigen und junge Menschen verantwortungsvoll anzuleiten, damit diese zukünftige gesellschaftliche Entwicklungen mitgestalten können. Um einen entscheidenden Mehrwert für die Gesellschaft zu generieren verfolgen wir das Ziel, in der Auseinandersetzung mit bedeutenden Fragen der Zukunft unser Profil weiter zu schärfen und stärker sichtbar zu machen. Eine sich dynamisch durch Globalisierung, Digitalisierung oder Klimawandel entwickelnde Welt erfordert große Flexibilität der AbsolventInnen. Wir statten dazu die Studierenden, neben dem notwendigen Wissen, mit jenen Kompetenzen aus, die sie fit für ihre persönliche Zukunft und die sich ändernden gesellschaftlichen Anforderungen machen.[1]

Wir betreiben Grundlagenforschung und angewandte Forschung auf Spitzenniveau, basierend auf den Grundsätzen wissenschaftlicher und ethischer Integrität und übernehmen in Lehre, Forschung, Wissenstransfer und Universitätsmanagement Verantwortung für nachhaltiges Handeln. Dies tun wir durch Berücksichtigung der ökologischen, ökonomischen und sozialen Dimension der Nachhaltigkeit und sind dabei ein Vorbild für die Gesellschaft. [2] Die dynamische Wirtschaftsentwicklung und die gesetzlichen Vorschriften stellen wiederkehrend hohe Ansprüche an die Leistungsbereitschaft und Anforderungen an die Organisation unseres professionell organisierten Forschungs- und Lehrbetriebs.

Eine der Anforderungen mit Vorbildwirkung ist der systematische Aufbau einer internen Kontrolle, mit Hilfe derer die Erfüllung gesetzlicher Vorgaben, die Zielerreichung und der Universitätsbetrieb im Allgemeinen sichergestellt wird.

Wir haben bereits in der Vergangenheit Anstrengungen unternommen, um interne Kontrollen und ein angemessenes Risikomanagement aufzubauen. Viele Kontrollen, Richtlinien und Darstellungen sind bereits vorhanden und in Kraft. Zur genauen Definition der internen Kontrolle ist jedoch ein gesamtes Regelwerk vorteilhaft. Das gegenständliche Handbuch zum Internen Kontrollsystem (IKS) soll diesen Zweck erfüllen. Es bildet den roten Faden bei der weiteren Entwicklung und soll uns bei der Steuerung des betrieblichen Geschehens helfen.

Der Rektor:
Riedler

[1] Siehe auch *Entwicklungsplan* i.d.g.F.
[2] Siehe auch *Leitbild* i.d.g.F.

2 Zusammenfassung

Aufgrund aktueller **Compliance-Anforderungen** insbesondere durch das UG i.d.g.F., dem Bundes-Public Corporate Governance Kodex i.d.g.F. sowie der Empfehlungen zu IKS-Mindeststandards der Universitäten des BMBWF nimmt die Bedeutung eines formalen Internen Kontrollsystem (IKS) zu.

Um dieser **Verantwortung** seitens des Rektorats gerecht zu werden, wurde das IKS bereits im Jahr 2005 in der Gebarungsrichtlinie verankert. Im Zuge der Überarbeitung 2018 bestellte das Rektorat einen externen IKS-Manager und beauftragte diesen mit der Koordination der Tätigkeiten zur Weiterentwicklung der IKS-Implementierung, der Durchführung von Risikomanagement-Workshops und der Erstellung und laufenden Aktualisierung des IKS-Handbuchs.

Bei der Wahl der anzuwendenden **Methoden** wurde darauf geachtet, international anerkannte Standards zu verwenden sowie die Empfehlungen zu IKS-Mindeststandards der Universitäten des BMBWF aus 2018 umzusetzen. So finden der weltweite de-facto Standard für IKS – das COSO-Rahmenmodell – sowie für die Risikobeurteilung, Bewertung und Darstellung ISO 31000 und der ÖNORM D 4902-2:2021-01 Anwendung.

Um den Grundätzen des UG betreffend Wirtschaftlichkeit, Sparsamkeit und Zweckmäßigkeit gerecht zu werden, wurde der **Umfang der Risikobeurteilung** eingegrenzt. Hierzu erarbeitete die AG IKS in einem Workshop gemeinsam mit dem IKS-Manager in Einklang mit den Empfehlungen des BMBWF einen Vorschlag mit den im ersten Schritt zu evaluierenden Einheiten. Der vorgeschlagene Umfang umfasste jene Einheiten, bei welchen eine Bündelung finanzwirtschaftlicher Prozesse und damit verbundener Risiken stattfindet und welchen die vom BMBWF genannten fünf Prozesse ([1] Beschaffung, [2] Finanzen [Budgetierung, Berichtswesen, Steuerung, Rechnungslegung, Veranlagung, etc.], [3] Drittmittel und Fundraising, [4] IT-Nutzung, [5] Personaladministration und Reisen) überwiegend zugeordnet werden können. Dieser Vorschlag wurde vom Rektorat genehmigt.

Nach Festlegung der zu beurteilenden Einheiten wurden mit den betroffenen Einheits-Leitungen und ausgewählten MitarbeiterInnen unter Anleitung des IKS-Managers **IKS-Workshops** durchgeführt. Im Rahmen dieser Workshops wurden die MitarbeiterInnen zum IKS geschult und gemeinsam mit ihnen unter Berücksichtigung der COSO-Struktur die Risiken, welche mit den finanzwirtschaftlichen Prozessen in Verbindung stehen, durch Brainstorming ermittelt. Anschließend wurden die Risiken nach Eintrittswahrscheinlichkeit und möglichem Schadensausmaß bewertet und ihnen eine Gesamtrisikobewertung zugewiesen. In weiterer Folge wurden den Risiken sofern möglich die gesetzten Kontrollaktivitäten zugeordnet und deren Effektivität bewertet. Je nach Reduktion des Risikos wurden die Kontrollaktivitäten als ausreichend bewertet oder müssen überarbeitet werden.

Die aktuellen **Ergebnisse** der Workshops zur Beurteilung der Risiken und Kontrollmaßnahmen wurden in der Risikokontrollmatrix (RKM) festgehalten, die hierfür angewendete Methodik und Vorgehensweise wurde im IKS-Handbuch beschrieben. Neben Richtlinien und Arbeitsanweisungen stellen das IKS-Handbuch und die RKM das Kernstück der **IKS-Dokumentation** dar. Sie dienen als Nachweis der Wirksamkeit des IKS und bilden die Grundlage für die weitere Berichterstattung:

- Das **IKS-Handbuch** gibt den allgemeinen Rahmen des IKS vor und beschreibt die angewandten Methoden, den Geltungsbereich, den Gesamtaufbau und -prozess und Rollen im IKS. Das IKS sieht verschiedene Rollen und Verantwortlichkeiten vor, wobei durch das IKS hinsichtlich Kontrollverantwortung und Kontrolldurchführung innerhalb der Uni Graz keine zusätzlichen Rollen definiert werden. Die IKS-Verantwortung ergibt sich originär aus der Geschäfts- bzw. Geschäftsprozessverantwortung. Das IKS-Handbuch wird vom Rektorat freigegeben und in Form einer Richtlinie publiziert.
- Die **Risikokontrollmatrix (RKM)** ergänzt das IKS-Handbuch mit aktuellen Detail-Dokumentationen zu Zuständigkeiten, evaluierten Einheiten, Risiken und Kontrollaktivitäten sowie korrespondierenden Richtlinien und Prozessen.

Das IKS unterliegt einer **kontinuierlichen Verbesserung**. Die Aktualisierung der Dokumente erfolgt einmal jährlich und wird vom externen IKS Manger / von der externen IKS-Managerin angestoßen.

Identifizierte Risiken und die getroffenen Kontrollaktivitäten werden durch die IKS-Managerin / den IKS-Manager einmal jährlich **an das Rektorat kommuniziert** und im Bedarfsfall erläutert. Dies umfasst die

- Übersicht über die Anzahl der Risken;
- Vorstellung der Risiken über dem Grenzrisiko;
- Erläuterung der Maßnahmen zur Risikoreduktion.

3 Einleitung

Die Uni Graz als Allgemeinuniversität versteht sich als eine internationale Forschungs- und Bildungseinrichtung mit Auftrag zur gesellschaftsrelevanten und gesellschaftsfördernden Forschung und Lehre[3]. Gegründet 1585 ist sie Österreichs zweitälteste Universität und eine der größten des Landes. Zahlreiche herausragende WissenschafterInnen, unter ihnen sechs Nobelpreisträger, haben hier gelehrt und geforscht. Mit rund 30.000 Studierenden und 4.700 MitarbeiterInnen trägt sie entscheidend zum pulsierenden Leben der steirischen Landeshauptstadt bei[4].

3.1 Über die Universität Graz

Unter Wahrung des Grundsatzes der Freiheit von Forschung und Lehre setzt sich die Uni Graz permanent mit sozialen, politischen und technologischen Entwicklungen auseinander. Zunehmende Flexibilisierung und Globalisierung sind dabei wesentliche Rahmenbedingungen. Profilbildung und Sichtbarkeit im europäischen und globalen Kontext sind für die Uni Graz von großer Bedeutung, wobei ein besonderes Merkmal der Universität die Positionierung im südosteuropäischen Raum darstellt.

Eine Beschreibung des Selbstverständnisses der Uni Graz, ihrer Grundprinzipien sowie ihrer Tätigkeiten ist im jeweils aktuellen *Leitbild* auf der Website der Uni Graz zu finden.

3.2 Zielsetzung

Der Zweck dieses IKS-Handbuchs ist es, eine transparente und einfach handzuhabende Form zu finden, um die internen Kontrollen der Uni Graz betreffend finanzwirtschaftlicher Angelegenheiten effizient zu gestalten. Es wird die Basis für das Interne Kontrollsystem (IKS) geschaffen, indem es – basierend auf international anerkannten Standards – eine einheitliche IKS-Vorgehensweise etabliert. Das IKS soll sicherstellen, dass Gesetze, ministerielle Empfehlungen und interne Richtlinien eingehalten werden, das Vermögen geschützt wird und die Universitätsziele erreicht werden. Das Rektorat soll damit in die Lage versetzt werden, das IKS und seine Wirksamkeit einzuschätzen und steuernd einzugreifen.

Ziel des IKS ist

- die Einhaltung des UG, insbesondere
  - leitende Grundsätze gemäß § 2 UG, wie Z 12 Wirtschaftlichkeit, Sparsamkeit und Zweckmäßigkeit,
  - Vorgaben betreffend finanzwirtschaftlicher Angelegenheiten (§§15, 16),
- die Erfüllung des Bundes-Public Corporate Governance Kodex 2017 (insbes. Abschnitte 9.1.3, 9.1.4, 15.1.1),
- den Empfehlungen zu IKS-Mindeststandards der Universitäten des Bundesministeriums für Bildung, Wissenschaft und Forschung (BMBWF) zu folgen,
- die Einhaltung der Gebarungsrichtlinie sicherzustellen und
- eine Basis zur Bewertung von Selbstbeurteilungen und Berichterstattung über Beurteilungsergebnisse betreffend finanzwirtschaftlicher Angelegenheiten zu schaffen.

[3] Siehe auch *Leistungsvereinbarung* i.d.g.F.

[4] Siehe auch das *Porträt der Universität* i.d.g.F. auf der Website der Uni Graz.

Insbesondere werden in Anlehnung an den international anerkannten Standard folgende Ziele verfolgt[5]:

- **Wirtschaftlichkeit:**
  Sicherstellung der Effektivität und Effizienz der Geschäftsprozesse
- **Berichterstattung:**
  Sicherstellung der Richtigkeit und Verlässlichkeit der internen und externen Berichterstattung
- **Regeleinhaltung:**
  Sicherstellung der Einhaltung der relevanten Gesetze und Verordnungen sowie der internen Richtlinien und Arbeitsanweisungen

Ein wirksamer IKS-Prozess ermöglicht, Risiken, die mit der Geschäftstätigkeit und den Abläufen verbunden sind, zu erkennen und zu diesen Risiken sinnvolle Kontrollen zu bestimmen. Das IKS ist elementarer Bestandteil der Geschäftsabläufe.

Es ist nicht Ziel des IKS

- Kontrollen um der Kontrollen willen durchzuführen – Grundsätzlich sind Kontrollen dazu da, die Auswirkungen bestehender Risiken durch entsprechende Maßnahmen zu reduzieren oder ganz zu vermeiden.
- Zusätzlichen Organisations- und Prozessaufwand zu generieren – es soll auf bereits bestehende Kontrolltätigkeiten aufgesetzt werden. Zusätzlicher Kontrollaufwand soll immer in einem gesunden Verhältnis zu dem daraus resultierenden Nutzen stehen.
- MitarbeiterInnen in ihren Tätigkeiten zu überwachen – Kontrollen sollen die MitarbeiterInnen bei der korrekten Ausführung ihrer Aufgaben unterstützen.

Dieses IKS-Handbuch soll das Rektorat sowie alle andere Bedienstete der Uni Graz in ihrer Eigenverantwortung betreffend finanzwirtschaftliche Angelegenheiten und IKS-Vorgaben unterstützen. Gleichzeitig dient es als Nachschlagewerk für alle Bedienstete der Uni Graz. Darüber hinaus soll das Kontrollbewusstsein geschärft und Führungskräfte angeregt werden, regelmäßig die Wirksamkeit und Effizienz der Geschäftsprozesse zu hinterfragen.

3.3 GELTUNGSBEREICH

Das IKS und das IKS-Handbuch gelten für die gesamte Uni Graz und umfassen sämtliche zentralen und dezentralen finanzwirtschaftlichen Angelegenheiten betreffend die Beschaffung, Finanzen (Budgetierung, Berichtswesen, Steuerung, Rechnungslegung, Veranlagung, etc.), Drittmittel und Fundraising, IT-Nutzung, Personaladministration und Reisen, udgl.

Betroffen sind alle Bedienstete (Führungskräfte und MitarbeiterInnen) der Uni Graz, welche mit zentralen oder dezentralen finanzwirtschaftlichen Angelegenheiten betraut wurden.

[5] Im September 1992 wurde in den USA ein Bericht des Committee of Sponsoring Organizations of the Treadway Commission (COSO) mit dem Titel “Internal Control - Integrated Framework” vorgestellt, der erstmals eine einheitliche Beurteilung der Wirksamkeit von IKS ermöglichen sollte. Darin wurden Ziele vorgegeben, die eine Organisation in Bezug auf das vorhandene IKS erreichen muss. Diese Ziele wurden in der 2013 erschienenen COSO-Überarbeitung deutlicher formuliert.

4 Grundlagen

Der Begriff und die Abgrenzung des IKS werden in der Literatur und Praxis national und international nicht einheitlich verwendet. Der Begriff des „Internen Kontrollsystems“ geht auf den in den USA entwickelten Begriff der „Internal Control“ zurück, der als Reaktion auf Betrugs- und Unterschlagungsfälle im amerikanischen Wirtschaftsleben entstand.

Ein IKS beinhaltet sämtliche Maßnahmen und Vorkehrungen mit dem Ziel der

- Sicherung des Betriebsvermögens;
- Effektivität und Effizienz in Geschäftsprozessen zur Verbesserung der betrieblichen Abläufe;
- Zuverlässigkeit und Vollständigkeit von finanziellen und operationellen Informationen sowie die ordnungsgemäße Gewährleistung der Zuverlässigkeit des Rechnungswesens;
- Einhaltung von Gesetzen, Bestimmungen und Verträgen (Compliance) zur Sicherung der Einhaltung der Geschäftspolitik.

Nach dieser Definition beschränken sich die Ziele des IKS ausschließlich auf die Gebiete der kaufmännischen Verwaltung.

4.1 Allgemeine IKS-Prinzipien

Die nachstehend angeführten grundlegenden Prinzipien finden im IKS ihre Anwendung:

- **Vier-Augen-Prinzip und Kontrollautomatik**
  Jeder wesentliche Prozess bzw. Arbeitsablauf unterliegt in einem gut definierten IKS einer Kontrolle durch eine Gegenkontrolle. Sofern möglich, ist auf den systematischen Einbau (z.B. IT-gestützter) automatisierten (System-)Kontrollen im Arbeitsablauf zu setzen.
- **Funktionstrennung**
  Die Funktionstrennung empfiehlt ausführende und verwaltende Tätigkeiten in einem IKS-relevanten Prozess zu trennen. So wird zum Beispiel empfohlen, dass Bestellungen nicht von der gleichen Person verbucht werden sollen.
- **Transparenz**
  Prozesse sollen klar definiert und dokumentiert werden. Dies gewährleistet gleichbleibende Arbeitsabläufe und ermöglicht einen Soll-Ist-Vergleich der tatsächlich gelebten Abläufe.
- **Mindestinformation sowie Mindestzugangs- und -zugriffsberechtigungen**
  Das Prinzip empfiehlt, dass MitarbeiterInnen nur jene Informationen, Zutritte und Verarbeitungsrechte zur Verfügung gestellt bekommen, die sie für Ihre Arbeitsabläufe benötigen.

4.2 Weitere IKS-Prinzipien

Darüber hinaus finden die in den Empfehlungen zu IKS-Mindeststandards der Universitäten des BMBWF aus 2018 definierten Prinzipien im IKS der Uni Graz ihre Anwendung[6]:

- **IKS als rollierender Prozess**
  Das IKS ist einer regelmäßigen und systematischen Überprüfung auf seine Funktionsfähigkeit, Wirksamkeit und Aktualität zu unterwerfen, 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 (Schadensausmaß und Eintrittswahrscheinlichkeit) stehen.

[6] Vgl. BMBWF Neugebauer, A. (2018): *Empfehlungen zu IKS-Mindeststandards der Universitäten*, GZ: BMBWF-11.111/0003-IV/7a/2018, S. 18-19.

4.3 Begriffsabgrenzungen

- **IKS und Risikomanagement**
  Risikomanagement und IKS sind untrennbar miteinander verbunden: 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 Prozesse) unabdingbar. Das Risikomanagement ist damit Grundvoraussetzung und Basis eines IKS. Interne Kontrollsysteme müssen bei Änderungen der Risikosituation angepasst werden
- **IKS und Compliance**
  Compliance–Management und IKS haben hinsichtlich der Zielsetzungen und Maßnahmen einen deutlichen Schnittmengenbereich; gemeinsam ist beiden die Zielsetzung der Einhaltung externer und interner Vorgaben. Wenn auch die Grundideen und damit der Fokus beider Konzepte etwas unterschiedlich sind, werden die Konzepte in der Praxis zunehmend gemeinsam betrachtet.

4.4 IKS – COSO Framework

Das *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) hat ein international anerkanntes und weit verbreitetes Rahmenwerk für den Aufbau und die Ausgestaltung eines IKS geschaffen. Zur Zielerreichung definiert COSO 2013 fünf Komponenten, die für ein effektives Kontrollsystem implementiert und wirksam sein müssen. Durch Zusammenwirken dieser Komponenten wird erreicht, dass wesentliche Falschdarstellungen vermieden oder erkannt und korrigiert werden können.

Jede der fünf im Standard vorgestellten internen Komponenten ist erforderlich, um das Ziel einer zuverlässigen Finanz-, Compliance- und Operations-Berichterstattung zu erreichen. Die Beurteilung, ob die interne Überwachung einer Organisation leistungsfähig ist, erfordert eine Ermessensentscheidung.

Die fünf Komponenten lauten (Components, siehe Abbildung 1):

1) Kontrollumfeld (Control Environment)
2) Risikobeurteilung (Risk Assessment)
3) Kontrollaktivitäten (Control Activities)
4) Information & Kommunikation (Information & Communication)
5) Überwachungsaktivitäten (Monitoring Activities)

Diese Komponenten sollen die Erreichung der drei Zielkategorien (Objectives) gewährleisten und umfassen alle Ebenen des Unternehmens (Levels).

Den fünf Komponenten sind im Standard 17 Prinzipien untergeordnet. Diese Prinzipien stellen die Grundsätze für ein effektives IKS dar. COSO wird national und speziell international vermehrt zum „de-facto“ Standard für den Aufbau und die Implementierung eines IKS.

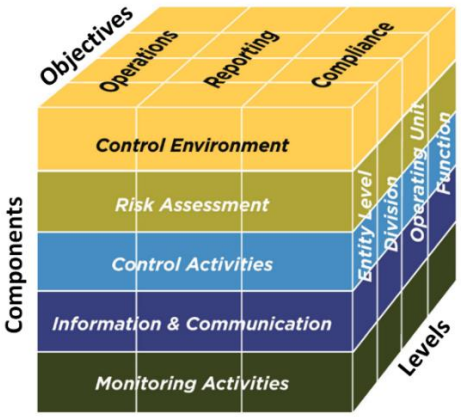

Abbildung 1: COSO-Würfel (Quelle: https://www.protiviti.com/sites/default/files/united_states/insights/updated-coso-internal-control-framework-faqs-third-edition-protiviti.pdf).

4.5 COSO-Prinzipien

4.5.1 Kontrollumfeld (5)

1) **Verpflichtung zu Integrität und ethischen Werten** – Die Organisation bekennt sich zu Integrität und ethischen Werten
2) **Ausübung der Aufsichtspflichten** – Das Überwachungsorgan ist unabhängig vom Management und überwacht die Entwicklung und Funktionsfähigkeit der internen Kontrollen.
3) **Etablierung von Strukturen, Befugnissen und Verantwortlichkeiten** – Das Management etabliert – unter der Aufsicht des Überwachungsorgans – Strukturen, Berichtslinien sowie angemessene Befugnisse und Verantwortlichkeiten zur Verfolgung der Unternehmensziele.
4) **Bekenntnis zu Kompetenz** – Die Organisation demonstriert ein Bekenntnis zur Einstellung, Entwicklung und Bindung von kompetenten Personen in Übereinstimmung mit den Unternehmenszielen.
5) **Durchsetzung der Rechenschaft** – Die Organisation überträgt Individuen die Rechenschaftspflicht für ihre internen Kontrollen zur Verfolgung der Unternehmensziele.

4.5.2 Risikobeurteilung (4)

6) **Spezifizierung von angemessenen Unternehmenszielen** – Die Organisation beschreibt zur Identifikation und Beurteilung damit verbundener Risiken die Unternehmensziele mit der notwendigen Klarheit.
7) **Identifizierung und Analyse von Risiken** – Die Organisation identifiziert mit der Erreichung von Unternehmenszielen verbundene Risiken auf Unternehmensebene und führt eine Risikoanalyse als Basis für die Risikosteuerung durch.
8) **Beurteilung von Betrugs-Risiken** – Die Organisation berücksichtigt die Möglichkeit für dolose Handlungen bei der Beurteilung der mit der Erreichung der Unternehmensziele verbundenen Risiken.
9) **Identifizierung und Analyse wesentlicher Veränderungen** – Die Organisation identifiziert und beurteilt Veränderungen, die einen wesentlichen Einfluss auf das IKS haben könnten.

4.5.3 Kontrollaktivitäten (3)

10) **Auswahl und Entwicklung von Kontrollaktivitäten** – Die Organisation selektiert und entwickelt Kontrollaktivitäten, die zur Risikoverminderung beitragen und die Erreichung der Unternehmensziele auf ein akzeptables Niveau bringen.
11) **Auswahl und Entwicklung genereller IT-Kontrollen** – Die Organisation selektiert und entwickelt generelle IT-Kontrollen zur Unterstützung der Erreichung von Unternehmenszielen.
12) **Implementierung von Regelungen und Verfahren** – Die Organisation implementiert Kontrollaktivitäten mit Hilfe von Regelungen zur Dokumentation von Erwartungen und -Verfahren zur Umsetzung der Regelungen.

Kontrollen sind eine Auswahl von Maßnahmen, die sicherstellen bzw. überwachen können, dass die Organisations- oder Prozessziele erreicht werden und das entsprechende Risiko vermieden bzw. hinreichend reduziert wird. Sie beschreiben im Detail, wie einzelne Kontrollschritte ausgeführt werden und wie dies zu dokumentieren ist. Es gilt der Grundsatz: Eine nicht dokumentierte Kontrolle gilt als nicht durchgeführte Kontrolle.

4.5.4 Information und Kommunikation (3)

13) **Nutzung relevanter Informationen** – Die Organisation beschafft oder generiert und nutzt relevante und qualifizierte Informationen zur Unterstützung der Funktionsfähigkeit von internen Kontrollen.
14) **Interne Kommunikation** – Die Organisation kommuniziert intern die notwendigen Informationen (inkl. der Ziele und Verantwortlichkeiten für interne Kontrollen) zur Unterstützung der Funktionsfähigkeit von internen Kontrollen.
15) **Externe Kommunikation** – Die Organisation kommuniziert mit externen Gruppen notwendige Informationen zur Unterstützung der Funktionsfähigkeit interner Kontrollen.

4.5.5 Überwachungsaktivitäten (2)

16) **Durchführung laufender und / oder gesonderte Beurteilungen** – Die Organisation selektiert, entwickelt und führt laufende und / oder gesonderte Beurteilungen durch zur Sicherstellung der Existenz und Funktionsfähigkeit aller Komponenten eines IKS.
17) **Evaluierung und Kommunikation von Kontrollschwächen** – Die Organisation evaluiert und kommuniziert interne Kontrollschwächen zeitnah an die für Korrekturmaßnahmen verantwortlichen Stellen und – soweit angemessen – die Unternehmensführung und das Überwachungsorgan.

4.6 RISIKOBEURTEILUNG

Unter *Risiko* versteht man Unsicherheiten in der Erreichung der Organisations- und Prozessziele aufgrund externer und interner Faktoren (Gefährdungen). Der Risikobegriff beschränkt sich wie das IKS insgesamt nicht auf Risiken der Rechnungslegung, sondern ist umfassend zu verstehen. Eine vereinfachte Risikoidentifizierung kann über die Frage erfolgen: „Was kann im Prozess falsch laufen?“.

Die Risikobeurteilung im zweiten Prozessschritt erfolgt durch Bewertung von Eintrittswahrscheinlichkeit und Auswirkung bzw. Schadenshöhe von Gefährdungen, um eine Grundlage für ihre Steuerung zu erhalten. Sowohl innewohnende (inhärente) Risiken als auch Restrisiken werden bewertet. Die Schwerpunkte liegen dabei auf den Kernbereichen der Organisation, die Bilanz- und GuV-Positionen sowie den Geschäftsprozessen. Die beste Grundlage ist die Kombination eines Risikokataloges und einer individuellen Risikoanalyse mit Risikobewertung.

4.6.1 Eintrittswahrscheinlichkeit und Schadenshöhe

Die Bewertung der Eintrittswahrscheinlichkeit und des zu erwartenden möglichen Schadens erfolgt durch Zuordnung zu je einer von fünf Bewertungsstufen entsprechend der Gliederung in der ONR 49002-2:2014. Diese Bewertungsstufen sind:

- **Eintrittswahrscheinlichkeit:** unwahrscheinlich, sehr selten, selten, möglich, häufig
- **Schadenshöhe:** unbedeutend, gering, spürbar, kritisch, katastrophal

Eine detaillierte tabellarische Beschreibung der jeweiligen Bewertungsstufen ist in der *Risikokontrollmatrix (RKM)* zu finden.

4.6.2 Risikoeinstufung

Tabelle 1 veranschaulicht die Risikoeinstufung nach der Einschätzung der Eintrittswahrscheinlichkeit und des zu erwartenden möglichen Schadens.[7]

Tabelle 1: Risikomatrix zur Risikoeinstufung.

Eintrittswahrscheinlichkeit		1 unbedeutend	2 gering	3 spürbar	4 kritisch	5 katastrophal
häufig	5	5	10	15	20	25
möglich	4	4	8	12	16	20
selten	3	3	6	9	12	15
sehr selten	2	2	4	6	8	10
unwahrscheinlich	1	1	2	3	4	5

Schadenshöhe

[7] Die Bedeutung der Begriffe sind in ONR 49000:2014 und ONR 49002–2:2014 Anhang A erläutert.

4.6.3 Risiko-Kategorie

Nach Bewertung von Eintrittswahrscheinlichkeit und Schadenshöhe wird anhand der Risikomatrix das Gesamtrisiko für die Organisation ermittelt. Die sich daraus ergebende Risikomaßzahl ist einer von drei der in Tabelle 2 angeführten Risiko-Kategorien zugeordnet.

Tabelle 2: Risiko-Kategorien.

Risikomaßzahl	Risiko-Kategorie	Erläuterung
1-4	Gering	Keine Risikoreduzierung nötig (zwischen Restrisiko und Grenzrisiko)
5-14	Signifikant	Risikoreduzierung notwendig (in der Nähe des Grenzrisikos bis leicht darüber)
15-25	Hoch	Risikoreduzierung dringend notwendig (über dem Grenzrisiko)

5 Vorgehensweise zur Umsetzung der Empfehlungen von IKS-Mindeststandards

5.1 Verantwortungsübernahme

Das Rektorat trägt die Verantwortung für die Umsetzung gesetzlicher Vorgaben, insbesondere jenen des UG i.d.g.F.[8] und des Bundes-Public Corporate Governance Kodex i.d.g.F.[9] sowie für die Umsetzung der Empfehlungen zu IKS-Mindeststandards der Universitäten[10].

Um seiner Verantwortung gerecht zu werden, wurde das IKS bereits im Jahr 2014 in der Gebarungsrichtlinie[11] verankert. Des Weiteren bestellt das Rektorat eine/n IKS-ManagerIn und beauftragt diese/n mit der Koordination der Tätigkeiten zur Weiterentwicklung der IKS-Implementierung, der Durchführung von Risikomanagement-Workshops und der laufenden Aktualisierung des IKS-Handbuchs. Die jeweils aktuelle Bestellung zur IKS-Managerin / zum IKS-Manager ist in der RKM zu finden.

5.2 Dokumentation IKS-relevanter finanzwirtschaftlicher Prozesse

In den Empfehlungen zu IKS-Mindeststandards der Universitäten des BMBWF aus 2018 werden fünf zentrale Prozesse identifiziert, die jedenfalls im IKS berücksichtigt sein müssen[12]:

1. Beschaffung
2. Finanzen (Budgetierung, Berichtswesen, Steuerung, Rechnungslegung, Veranlagung, etc.)
3. Drittmittel und Fundraising
4. IT-Nutzung
5. Personaladministration und Reisen

[8] Siehe auch *Bundesgesetz über die Organisation der Universitäten und ihre Studien (Universitätsgesetz 2002 – UG)*.
[9] Bundeskanzleramt (2017): *Bundes Public Corporate Governance Kodex 2017(B-PCGK 2017). Grundsätze der Unternehmens- und Beteiligungsführung im Bereich des Bundes*, Wien.
[10] BMBWF Neugebauer, A. (2018): *Empfehlungen zu IKS-Mindeststandards der Universitäten*, GZ: BMBWF-11.111/0003-IV/7a/2018.
[11] Siehe *Richtlinie des Rektorats für die Gebarung* i.d.g.F.
[12] Vgl. BMBWF Neugebauer, A. (2018): *Empfehlungen zu IKS-Mindeststandards der Universitäten*, GZ: BMBWF-11.111/0003-IV/7a/2018, S. 7-8.

Diese IKS-relevanten finanzwirtschaftlichen Prozesse umfassen die gesamte Uni Graz und werden über die verschiedenen Fakultäten und akademische Einheiten, Verwaltungseinheiten sowie universitäts- und fakultätsübergreifende Leistungsbereiche (in der Folge verkürzt als „Einheiten“ bezeichnet) hinweg gelebt. Die Prozessverantwortung und fachliche Expertise zu den Risiken und Kontrollmaßnahmen in Zusammenhang mit diesen Prozessen liegt bei den jeweiligen Leitungen der Einheiten. Die Prozesse werden mittels entsprechender Richtlinien gelenkt.

Das Kernstück der IKS-Dokumentation bilden das gegenständliche IKS-Handbuch und die RKM, welche auch die Grundlage für die weitere Berichterstattung bilden:

- Das IKS-Handbuch gibt den allgemeinen Rahmen des IKS vor und beschreibt die angewandten Methoden, den Geltungsbereich und den Gesamtaufbau und -prozess. Dieses wird vom Rektorat freigegeben.
- Die RKM ergänzt das IKS-Handbuch mit aktuellen Detail-Dokumentationen zu Zuständigkeiten, evaluierten Einheiten, Risiken und Kontrollaktivitäten sowie korrespondierenden Richtlinien und Prozessen.

5.3 Evaluierung der Risiken und Kontrollen

Um den Grundätzen des UG betreffend Wirtschaftlichkeit, Sparsamkeit und Zweckmäßigkeit gerecht zu werden, wurde im Rahmen eines IKS-Workshops am 26. Juni 2018 der Bereich zur primären Dokumentation und Risikobeurteilung eingegrenzt. Dies erfolgte durch die Arbeitsgruppe IKS (AG IKS) gemeinsam mit dem IKS-Manager und in Einklang mit den Empfehlungen zu IKS-Mindeststandards des BMBWF. Der im ersten Schritt zu evaluierende Umfang wurde auf jene Einheiten beschränkt, bei welchen eine Bündelung finanzwirtschaftlicher Prozesse und damit verbundener Risiken stattfindet und welchen die vom BMBWF genannten fünf Prozesse überwiegend zugeordnet werden können. Darüberhinausgehend wurden zusätzliche Einheiten berücksichtigt, deren Prozesse ebenfalls als für das IKS relevant erachtet wurden.

Anschließend wurden mit den betroffenen Einheits-Leitungen und ausgewählten MitarbeiterInnen unter Anleitung des IKS-Managers Workshops durchgeführt und die Risiken und Kontrollmaßnahmen, welche mit den finanzwirtschaftlichen Prozessen in Verbindung stehen, dokumentiert.

- Zur Erstellung einer Systematik und transparenten Vorgehensweise für die internen Kontrollen wurde entsprechend den Empfehlungen des BMBWF der Aufbau des COSO-Rahmenmodells gewählt. [13] Für Methoden der Risikobeurteilung, Bewertung und Darstellung wurden die ISO 31000 und die ÖNORM D 4902-2:2021-01 zur Anwendung herangezogen.
- Im Rahmen dieser Workshops wurden die MitarbeiterInnen zum IKS geschult und gemeinsam mit ihnen unter Berücksichtigung der COSO-Struktur die möglichen Risiken durch Brainstorming ermittelt.
- Anschließend wurden die Risiken nach Eintrittswahrscheinlichkeit und möglichem Schadensausmaß bewertet und ihnen eine Gesamtrisikobewertung zugewiesen. Diese Bewertung wurde in der RKM dokumentiert.[14]
- In weiterer Folge wurden den Risiken die gesetzten Kontrollaktivitäten zugeordnet und deren Effektivität bewertet. Je nach Reduktion des Risikos wurden die Kontrollaktivitäten als ausreichend bewertet oder müssen überarbeitet werden.

[13] Vgl. BMBWF Neugebauer, A. (2018): *Empfehlungen zu IKS-Mindeststandards der Universitäten*, GZ: BMBWF-11.111/0003-IV/7a/2018, S. 15-16.
[14] Vgl. BMBWF Neugebauer, A. (2018): *Empfehlungen zu IKS-Mindeststandards der Universitäten*, GZ: BMBWF-11.111/0003-IV/7a/2018, S. 11.

6 IKS Aufbau und Prozess

Die Uni Graz soll die Ordnungsmäßigkeit des Rechnungswesens mit ausreichender Gewähr sicherstellen können. Des Weiteren soll sichergestellt werden, dass die Prinzipien des IKS eingehalten und gesetzliche und inneruniversitäre Vorgaben zu finanzwirtschaftlichen Angelegenheiten erfüllt werden. Das IKS ist ein Führungsinstrument in den Diensten der Planung, Durchführung und laufenden Überwachung der Arbeits- und Betriebsabläufe. Aufbauend auf den vorhandenen Rahmenbedingungen werden unter Berücksichtigung der COSO-Struktur die Risiken bearbeitet und Kontrollschritte vereinbart und geregelt. Diese Kontrollen werden systematisch unter Einhaltung von Effizienz und Effektivität geprüft. Die Überwachung der Kontrollen ist Einheits-übergreifend und prozessbezogen. Ein weitergehender Ansatz ist es, Überwachungsinstrumente einzurichten, die eine proaktive, zeitgerechte und effiziente Überwachung der IKS-Kontrollen ermöglichen.

Nachfolgend wird die Implementierung des IKS der Uni Graz erläutert. Für die Umsetzung des IKS in den einzelnen Einheiten gibt es keine davon abweichenden Vorgaben.

6.1 KONTROLLUMFELD

6.1.1 Uni Graz allgemein

Die nachfolgend beschriebene Definition des Kontrollumfelds gilt für alle IKS-Bereiche der Uni Graz und wird für die Einheiten nicht erneut dargestellt.

6.1.1.1 Rahmenbedingungen

Mit dem Universitätsgesetz 2002 und auf dieser Basis erlassene Verordnungen sowie dem Bundes-Public Corporate Governance Kodex 2017 (insbes. Abschnitte 9.1.3, 9.1.4, 15.1.1) wurden die **rechtlichen Rahmenbedingungen** für die Etablierung eines IKS geschaffen. Zudem veröffentlichte das BMBWF Empfehlungen zu IKS-Mindeststandards der Universitäten, an welchen sich die Uni Graz orientiert.

Weitere Rahmenbedingungen, welche die Leitung und den inneren Aufbau der Universität betreffen, sind im 2. Abschnitt des UG geregelt, insbesondere:

- Universitätsrat
- Senat
- Rektorat

Inneruniversitäre Rahmenbedingungen für das IKS ergeben sich durch Verordnung (Satzung), mit welcher die Universität die erforderlichen Ordnungsvorschriften im Rahmen der Gesetze und Verordnungen selbst erlässt und publiziert (Mitteilungsblätter)[15]. Dies umfasst die Verpflichtung zu Integrität und ethischen Werten, Richtlinien und systematische interne Kontrollen, über die die Uni Graz bereits verfügt, und welche als Gewohnheit und Regelmäßigkeit etabliert sind, insbesondere:

Organisatorische Strukturen:

- Arbeitskreis für Gleichbehandlungsfragen (AKGL)
- Interne Revision
- Ethikkommission

Lenkungsdokumente:

- Satzung
- Leitbild, Universitätsstrategie, Forschungsprofil
- Compliance-Richtlinie

Die Uni Graz bekennt sich zur Einstellung, Entwicklung und Bindung von **kompetenten Personen** in Übereinstimmung mit dem Leitbild und den Universitätszielen gemäß Entwicklungsplan.

[15] Sie auch die Beschreibung von *Organisation & Struktur* i.d.g.F. auf der Website der Uni Graz.

6.1.1.2 Organisation und Struktur

Die Universität Graz ist eine juristische Person des öffentlichen Rechts und gliedert sich in die oberste Leitung, Organisationseinheiten – die Fakultäten – die Verwaltung der Universität sowie universitäts- und fakultätsübergreifende Leistungsbereiche.[16] Rektorat, Universitätsrat und Senat bilden die obersten Leitungsorgane der Universität.[17]

Die Leitungsorgane der Uni Graz etablieren entsprechend ihren gesetzlichen Befugnissen Strukturen, Berichtswesen sowie angemessene Kompetenzen und Verantwortlichkeiten zur Verfolgung der Universitätsziele.

6.1.1.3 Rollen und Verantwortlichkeiten

Das IKS sieht verschiedene Rollen und Verantwortlichkeiten vor, wobei durch das IKS hinsichtlich Kontrollverantwortung, Kontrolldurchführung sowie Überwachungstätigkeiten innerhalb der Uni Graz keine zusätzlichen Rollen definiert werden. Die IKS-Verantwortung ergibt sich originär aus der Geschäfts- bzw. Geschäftsprozessverantwortung (siehe Tabelle 3). Im Rahmen der Überwachungs- und Berichterstattungsprozesse zur IKS-Wirksamkeit ergeben sich jedoch zusätzliche Aufgaben. So überwachen die mit IKS-Aufgaben betrauten Personen die Entwicklung und Funktionsfähigkeit der internen Kontrollen und sind in dieser Funktion rechenschaftspflichtig. Zusätzliche Rollen ergeben sich jedoch hinsichtlich beratender Tätigkeiten zu IKS-Angelegenheiten (siehe Tabelle 4).

Tabelle 3: Verantwortung im IKS.

Ebenen	Rollen
Uni Graz	Oberste Leitungsorgane der Uni Graz (Rektorat, Universitätsrat und Senat)
Rektorat	RektorIn, VizerektorInnen
Einheiten	Leitungen der Fakultäten und akademische Einheiten, Verwaltungseinheiten, universitäts- und fakultätsübergreifende Leistungsbereiche

Tabelle 4: Beratende Rollen im IKS

IKS-Rolle	Zuteilung
IKS-ManagerIn	Externe Dienstleistung
AG IKS	Ausgewählte Einheits-Leitungen

Im Folgenden werden die Rollen und Verantwortlichkeiten und die damit verbundenen Aufgaben aller im IKS Überwachungsprozess beteiligten Personen erläutert.

[16] Eine aktuelle Übersicht über die Organisation und Struktur ist im *Organisationsplan* der Uni Graz i.d.g.F. zu finden.

[17] Sie auch die Beschreibung von *Organisation & Struktur* i.d.g.F. auf der Website der Uni Graz.

Rektorat

Die Gesamtverantwortung für das IKS der Uni Graz trägt das Rektorat, welches eine/n externe/n IKS-ManagerIn bestellt und die Besetzung der Arbeitsgruppe Internes Kontrollsystem (AG IKS) festlegt.

Das Rektorat ist verantwortlich für:

- die Bereitstellung des Budgets zur Aufrechterhaltung und Weiterentwicklung des IKS;
- die regelmäßige Beurteilung der Existenz und Wirksamkeit des IKS;
- die kritische Durchsicht und Freigabe der Berichterstattung;
- die Festlegung der von der Risikobeurteilung zu erfassende Einheiten auf Basis der Empfehlung der AG IKS;
- die Durchführung eines regelmäßigen, jedoch mindestens einmal jährlichen Informationsaustauschs zu IKS-Sachverhalten, insbesondere den Risiken mit der IKS-Managerin / dem IKS-Manager – bei Bedarf auch ad hoc;
- die Überwachung der Umsetzung notwendiger Maßnahmen und IKS-Verbesserungen;
- ggf. die Beauftragung der Überprüfungen des IKS durch die Interne Revision oder Externe (Sachverständige, Abschlussprüfer, andere Wirtschaftsprüfer).

Für zentrale Themen und die Gesamtmethodik ist **das für Finanzen zuständige Rektoratsmitglied** verantwortlich und wird durch die IKS Managerin / den IKS-Manager unterstützt.

IKS-ManagerIn

Die externe IKS-Managerin / Der externe IKS-Manager wird vom Rektorat bestellt und koordiniert die IKS-Aktivitäten der Uni Graz übergreifend. Sie / Er ist verantwortlich für:

- die jährliche Berichterstattung an das Rektorat und Mitwirkung an der Vorbereitung für das Rektoratsmeeting;
- die Erarbeitung einer Empfehlung der von der Risikobeurteilung zu betrachtenden Einheiten in Zusammenarbeit mit der AG IKS;
- die Koordination und Durchführung der Risikobeurteilung und Bewertung der Kontrollaktivitäten im Rahmen von einmal jährlich stattfindenden Workshops. Hierbei wird sie/er durch die Leitungen der Einheiten unterstützt;
- Methodenkompetenz: sie/er gibt die fachliche Ausgestaltung des IKS vor und ist zudem verantwortlich für die Erarbeitung, Weiterentwicklung und Kommunikation der universitären IKS-Methodik und der Regelungsprozesse;
- die Unterstützung (Hilfestellung) des Rektorats und der Einheits-Leitungen bei (methodischen) Fragen;
- die Sicherstellung der Qualität im IKS-Umsetzungsprozesses und der Berichterstattung (Qualitätssicherung);
- die Aktualisierung der RKM.

AG IKS

Die AG IKS wird aus ausgewählten Einheits-Leitungen zusammengesetzt und wird vom für Finanzen zuständigen Rektoratsmitglied bestimmt. Sie erfüllt folgende Aufgaben:

- Teilnahme an jährlich stattfindenden Workshops zur Weiterentwicklung des IKS und des IKS-Handbuchs,
- Erarbeitung von Empfehlungen an das Rektorat betreffend der mittels Risikobeurteilung zu evaluierenden Bereiche (das Rektorat entscheidet über den Risikoerhebungsbereich). Diese werden jährlich und zeitlich mit der Wirtschaftsprüfung korrespondierend (September bis Dezember) erarbeitet.

Einheits-Leitung (Leitung der Fakultät oder akademischen Einheit, der Verwaltungseinheit oder des universitäts- und fakultätsübergreifenden Leistungsbereichs)

Die Einheits-Leitung ist die Ansprechperson für die IKS-Aktivitäten in ihrem Wirkungsbereich und koordiniert diese. Sie unterstützt die IKS-Managerin / den IKS-Manager bei der Risikobeurteilung und Bewertung der Kontrollaktivitäten und ist verantwortlich für die

- Aufsicht, Zielsetzung, Einrichtung und Führung eines wirksamen IKS und Anpassung der IKS-Vorgehensweisen entsprechend der für die Uni Graz festgelegten IKS-Methodik innerhalb ihres Wirkungsbereichs;
- Sicherstellung der Prozessqualität und der Wirksamkeit des IKS sowie die Identifikation von Verbesserungsbedarf auf Prozess- und Kontrollebene;
- Festlegung und Umsetzung von Maßnahmen auf Basis des identifizierten Verbesserungsbedarfs, beispielsweise Änderung bestehender Kontrollen oder Implementierung neuer Kontrollen;
- (punktuelle) Qualitätssicherung der IKS-Dokumentation;
- Mitwirkung bei der Risikoerhebung und Richtliniensteuerung;
- Förderung der Kommunikation zwischen den Einheits-Leitungen und MitarbeiterInnen;
- verantwortungsbewusste Durchführung der Kontrollmaßnahmen bei allen Beteiligten des Wirkungsbereichs, d. h. die Forderung und Förderung eines angemessenen Kontrollbewusstseins.

6.1.2 Umsetzung in den Einheiten

Siehe Beschreibung des Kontrollumfelds unter Abschnitt 6.1.1.

6.2 RISIKOBEURTEILUNG

6.2.1 Uni Graz allgemein

Der **Risikomanagementprozess** wird dem Abschnitt 4.6 entsprechend einmal jährlich durchgeführt, um mit den Zielen der Universität[18] verbundene neue Risiken zu identifizieren bzw. bekannte Risiken auf deren Eintrittswahrscheinlichkeit und Schadenshöhe zu evaluieren. Die daraus entstehende Bewertung ergibt die RKM. Identifizierte Risiken werden mittels Prozesse, Richtlinien und Vorgehensweisen behandelt (Kontrollaktivitäten). Um den Grundätzen zu Wirtschaftlichkeit, Sparsamkeit und Zweckmäßigkeit gerecht zu werden, liegt die Priorität der Risikobeurteilung bei jenen Einheiten mit den höchsten wirtschaftlichen Risiken und bei der höchst möglichen Schadenshöhe.

Der Risikomanagementprozess wird von der IKS-Managerin / vom IKS-Manager durch aktive Kommunikation an die AG IKS und die Einheits-Leitungen mit aktuellen Informationen angestoßen. Eingeleitet wird er mit der Festlegung der zu evaluierenden Einheiten. Zu diesem Zweck erarbeitet die AG IKS gemeinsam mit der IKS-Managerin / dem IKS-Manager eine Empfehlung mit den zu evaluierenden Einheiten und unterbreitet diesen Vorschlag dem Rektorat, welches endgültig über den zu evaluierenden Bereich entscheidet.

Anschließend werden unter Anleitung der IKS-Managerin / des IKS-Managers gemeinsam mit den Einheits-Leitungen Workshops durchgeführt, um neue Risiken zu identifizieren bzw. bekannte Risiken auf deren Eintrittswahrscheinlichkeit und Schadenshöhe zu evaluieren.

Die Ergebnisse der Risikobeurteilung werden der AG IKS vorgestellt und nach deren Rückmeldung an das Rektorat kommuniziert.

Die Risiken für die Uni Graz sind in der RKM zu finden.

[18] siehe Abschnitt 6.1.1.1 Rahmenbedingungen und Abschnitt 3.2 Zielsetzung.

6.2.2 Umsetzung in den Einheiten
Die Risikobeurteilungen der einzelnen Einheiten sind in den jeweiligen Reitern der RKM zu finden.

6.2.3 Beteiligungsverwaltung
Risiken in Verbindung mit Gesellschaften, bei welchen die Uni Graz eine steuernde Beteiligung innehat, werden im Rahmen der Risikobeurteilung mitbetrachtet.

6.3 KONTROLLAKTIVITÄTEN

6.3.1 Uni Graz allgemein
Die Uni Graz selektiert, entwickelt und implementiert Kontrollaktivitäten, die zur Vermeidung oder Reduktion von Risiken auf ein akzeptables Niveau beitragen. Das Funktionieren der internen Kontrolle hängt von den MitarbeiterInnen ab, die ihre Aufgaben und Zuständigkeiten, ebenso wie die Grenzen ihrer Kompetenzen genau kennen. Die Umsetzung der Regelungen erfordert intensive Kommunikation zwischen den Leitungsebenen und den MitarbeiterInnen.

Die Kontrollaktivitäten der Uni Graz sind in der RKM zu finden.

6.3.2 Umsetzung in den Einheiten
Die Kontrollaktivitäten der einzelnen Einheiten sind in den jeweiligen Reitern der RKM zu finden.

6.4 INFORMATION UND KOMMUNIKATION

6.4.1 Uni Graz allgemein
Die Uni Graz beschafft oder generiert und nutzt relevante und qualifizierte Informationen und/oder kommuniziert notwendige Informationen zur Unterstützung des IKS. So werden identifizierte Risiken und die getroffenen Kontrollaktivitäten durch die IKS-Managerin / den IKS-Manager einmal jährlich an das Rektorat kommuniziert und im Bedarfsfall erläutert. Dies umfasst die

- Übersicht über die Anzahl der Risken;
- Vorstellung der Risiken über dem Grenzrisiko;
- Erläuterung der Maßnahmen zur Risikoreduktion.

Als Vorbereitung für das Rektoratsmeeting zum Thema IKS erfolgt eine Vorabstimmung der Präsentation zwischen der IKS-Managerin / dem IKS-Manager und dem für Finanzen zuständigen Rektoratsmitglied.

Das Rektorat kann wesentliche Ergebnisse an den Universitätsrat berichten, darüber hinaus ist ein Bericht erforderlich, wenn daraus Entscheidungen des Universitätsrats aufgrund der gesetzlichen und/oder der Gebarungsrichtlinie notwendig sind. Dabei kann das Rektorat sich der Unterstützung der IKS-Managerin / des IKS-Managers bedienen.

Informationen betreffend das IKS können von den Einheits-Leitungen jederzeit an die IKS-Managerin / den IKS-Manager kommuniziert werden. Spätestens zum Zeitpunkt der einmal jährlich stattfindenden Workshops erfolgt ein Informationsaustausch zwischen IKS-ManagerIn und Einheits-Leitungen, im Rahmen derer für das IKS erforderliche Informationen eingeholt und/oder kommuniziert werden.

Das IKS-Handbuch wird in Form einer Richtlinie publiziert.

6.4.2 Umsetzung in den Einheiten
Siehe die Beschreibung in Abschnitt 6.4.1.

6.5 ÜBERWACHUNGSAKTIVITÄTEN

6.5.1 Uni Graz allgemein

Die Uni Graz selektiert, entwickelt und führt Beurteilungen zur Funktionsfähigkeit des IKS durch. Dafür werden eigens für die jeweilige Überwachungsaktivitäten entsprechende Evaluierungsmethoden (bspw.: Wirksamkeitstest, Analyse der Kontrollergebnisse, Schlussfolgerungen, etc.) und Zeiträume festgelegt, durchgeführt und dokumentiert. Interne Kontrollschwächen werden evaluiert und zeitnah im Rahmen der geltenden Berichtswege kommuniziert.

Die Überwachungsaktivitäten samt deren Ausgestaltung und Dokumentationserfordernisse der Uni Graz sind in der RKM zu finden.

6.5.2 Umsetzung in den Einheiten

Die Überwachungsaktivitäten der einzelnen Einheiten sind in den jeweiligen Reitern der RKM zu finden.

6.6 IKS-DOKUMENTATION

Die IKS-Dokumentation dient als Nachweis der Wirksamkeit des IKS. Sie bildet die Grundlage für eine Prüfung durch die Interne Revision sowie ggf. für andere externe Prüfungen. Im Rahmen der IKS-Dokumentation muss daher sichergestellt sein, dass die IKS-relevanten Unterlagen angemessen abgelegt und aktuell sind. Unter IKS-relevante Unterlagen fallen:

- Gegenständliches IKS-Handbuch
- Risikokontrollmatrizen (RKM)

Die IKS Managerin / Der IKS-Manager verantwortet die angeführten Dokumente und hat die Gesamtübersicht über diese. Nach den abgehaltenen Workshops werden der AG IKS die gesamte RKM und das IKS-Handbuch zur Verfügung gestellt. Den Einheits-Leitungen werden auf Nachfrage die sie betreffenden Ausschnitte der RKM bereitgestellt. Das IKS-Handbuch wird bei Änderungen erneut verlautbart.

In Vorbereitung auf die jährlichen Workshops erhalten alle betroffenen Einheits-Leitungen einen aktuellen Auszug der sie betreffenden RKM-Informationen.

Bei unterjährigen Änderungen erhält die AG IKS die jeweils aktuelle RKM.

6.6.1 Dokumentenrevision

Es ist jährlich zu überprüfen, ob gegenständliches IKS-Handbuch und die RKM noch aktuell sind. Dies erfolgt gemäß Abschnitt 6.2.1. Die Beschreibung der Risiken und Kontrollen müssen stets den tatsächlichen Gegebenheiten entsprechen. Wenn sich Gegebenheiten ändern, ist die IKS-Managerin / der IKS-Manager zu kontaktieren. Jedenfalls erfolgt eine entsprechende Anpassung der Dokumentation im Zuge der Workshops.

6.6.2 Dateistruktur

IKS-Handbuch und die RKM werden von der IKS-Managerin / vom IKS-Manager extern verwaltet und für notwendige Termine in der aktuellen Version bereitgestellt.

Für die Speicherung dieser Unterlagen ist folgende Namenskonvention einzuhalten:

UniGraz_Dokument_Jahr-Version_Name der Einheit

Beispiele:

RKM:	UniGraz_RKM_2018-V_Einheit.xlsx