MITTEILUNGSBLATT
DER
Medizinischen Universität Innsbruck

Internet: http://www.i-med.ac.at/mitteilungsblatt/

Studienjahr 2021/2022 | Ausgegeben am 8. Februar 2022 | 19. Stück

Medieninhaberin, Herstellerin, Herausgeberin und Redaktion: Medizinische Universität Innsbruck.
Anschrift, Verlags- und Herstellungsort: Innrain 52, A-6020 Innsbruck.

72. Leitfaden für das Interne Kontrollsystem (IKS)

Das Rektorat hat am 27.01.2022 den Leitfaden für das Interne Kontrollsystem (IKS) beschlossen (Anlage).

Für das Rektorat:

Mag.ª Manuela Groß
Vizerektorin für Finanzen und IT

Leitfaden für das Interne Kontrollsystem (IKS)

Medizinische Universität Innsbruck

Stand 26.01.2022

Inhaltsverzeichnis

Präambel

Die Medizinische Universität Innsbruck (MUI) ist darauf ausgerichtet, in Forschung und forschungsgeleiteter akademischer Lehre neue wissenschaftliche Erkenntnisse hervorzubringen. Sie erfüllt darüber hinaus ihre gesetzlich verpflichtende Mitversorgung von PatientInnen am Landeskrankenhaus Innsbruck mit seinem spitzendmedizinischen Anspruch. Ebenso ist sie sich als öffentliche Universität ihrer gesellschaftspolitischen Verantwortung bewusst.

In ihrer jährlichen Berichterstattung bekennt sich die MUI zur Einhaltung der Grundsätze des Bundes Public Corporate Governance Kodex 2017 (B-PCGK). Dazu gehört auch die Ausgestaltung (Konzeption, Implementierung, laufende Anpassung und Weiterentwicklung) eines angemessenen und wirksamen Internen Kontrollsystems (IKS), das die effektive Verfolgung der Geschäftsprozesse mithilfe von Kontrollen zur Risikominimierung und -vermeidung zum Ziel hat. Grundlage dafür bilden die vom Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF) zu IKS-Mindeststandards der Universitäten am 25.10.2018 herausgegebenen Empfehlungen.

Die Medizinische Universität Innsbruck (im Folgenden: MUI) bekennt sich zu einem diesem Leitfaden entsprechenden funktionsfähigen Internen Kontrollsystem, welches den Anforderungen der Universität entspricht und von allen Organisationseinheiten einzuhalten ist.

1. Allgemeines

Das interne Kontrollsystem ist ein in die Arbeits- und Betriebsabläufe der Universität eingebetteter Prozess, der von den leitenden Organen sowie den Mitarbeiterinnen/den 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.

Die Bestandteile des IKS an der MUI setzen sich aus den Kontrollen und deren systematischer Dokumentation zusammen, die laufend bzw. in regelmäßigen Abständen in strukturierter Form durchgeführt werden.

Grundlage für ein funktionierendes IKS sind strategische Vorgaben für die Organisation durch die Leitungsebene sowie ein laufendes Risikomanagement.

In erster Linie sind die Führungskräfte für das IKS im jeweiligen Bereich verantwortlich. Sie haben dafür zu sorgen, dass vorbeugende oder korrektive Maßnahmen gesetzt werden und die MitarbeiterInnen die erforderlichen prozessabhängigen als auch prozessunabhängigen Kontrollen durchführen und dokumentieren. Wie diese Maßnahmen gesetzt und deren Effektivität kontrolliert werden sollen, wird im Folgenden abgebildet bzw. ist Inhalt dieses IKS-Leitfadens.

Erforderlich für die Umsetzung des IKS ist es, Kontrollen in die Organisationsführung zu integrieren und zu dokumentieren. Interne Kontrollen sind dabei in die laufenden Prozesse zu integrieren. Deshalb ist es essentiell innerhalb eines Prozesses Funktionstrennungen vorzusehen, die gewährleisten, dass Entscheidung, Ausführung und Kontrolle nicht in der Hand einer Person oder einer Organisationseinheit liegen. Das Vier-Augen-Prinzip für sensible, insbesondere gebarungsrelevante Vorgänge spielt hier ebenso eine Rolle wie die Definition von Befangenheits- und Unvereinbarkeitsregelungen.

Eine laufende Aktualisierung und Weiterentwicklung des IKS im Sinne einer Analyse von Mängeln und Anpassungsnotwendigkeiten zählen als Mindestanforderungen an ein IKS. Dabei ist stets das Kosten-Nutzen-Verhältnis auszugestalten: die Dichte der Prozessvorgaben und Kontrollelementen ist an den Kriterien Risiko und Zweckmäßigkeit auszurichten.

1.1. Begriffsabgrenzungen

IKS und Risikomanagement

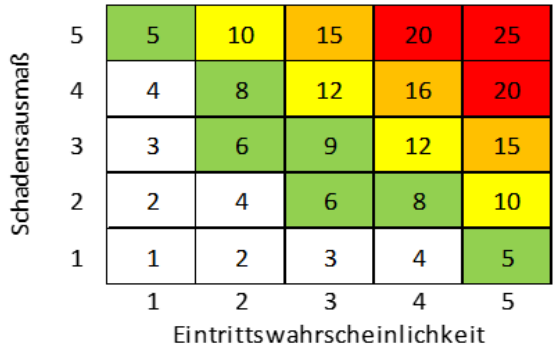
IKS und Risikomanagement sind untrennbar miteinander verbunden. Das IKS soll sicherstellen, dass das Erreichen der Organisations- bzw. Universitätsziele nicht durch interne und externe Risiken gefährdet wird. Zur Beurteilung der Qualität eines IKS ist die Kenntnis der Risiken der geprüften Organisation (der geprüften Prozesse) unabdingbar. Das Risikomanagement ist damit Grundvoraussetzung und Basis eines IKS.
Der Ablauf des Risikomanagementprozesses orientiert sich an den ISO Normen – u.a. an der ISO 31000 Risikomanagement somit an Leitlinien, die den Umgang mit Risiken in einer Organisation beschreiben.

Interne Kontrollsysteme müssen bei Änderungen der Risikosituation angepasst werden.

Die standardisierte Beurteilung der Risiken an der MUI wird über eine Risikomatrix mit 5 Toleranzbereichen abgebildet:

Risikobewertung (Risikowert)

Schadensausmaß		Eintrittswahr-scheinlichkeit		Risikowert		
1-unwesentlich		1-fast nie		von 1 bis 4	Sehr gering (negierbar)	
2-niedrig	x	2-selten	=	über 4 bis 9	Gering (nicht negierbar)	
3-moderat		3-gelegentlich		über 9 bis 12	Mittel (tolerierbar)	
4-beträchtlich		4-öfters		über 12 bis 16	Hoch (handhabbar)	
5-massiv		5-häufig		über 16 bis 25	Sehr hoch (spürbar)	



IKS und Interne Revision

Eine wichtige Aufgabe der Internen Revision ist die Prüfung des IKS; vor diesem Hintergrund wird die Interne Revision daher als außerhalb des IKS stehend angesehen.

1.2. Angewandte Standards

Das Modell des Committee of Sponsoring Organisations of the Treadway Commission (COSO, Internal Control — Integrated Framework, Mai 2013) gilt als weltweit anerkannter IKS-Standard.

Auch dem Leitfaden des BMBWF folgend wird dem IKS der MUI das Modell COSO IC zugrunde gelegt. Der COSO-Würfel soll die Gesamtheit der Dimensionen des IKS im Unternehmen repräsentieren, die sich in Ziele, Komponenten und Unternehmenseinheiten gliedern. Hierbei erfolgt eine Anpassung an die Erfordernisse bzw. Rahmenbedingungen der MUI – siehe dazu im Konkreten die Darstellung und Beschreibung in Beilage 3.

1.3. IKS-Prinzipien

- Transparenz-Prinzip, Grundsatz der Nachvollziehbarkeit:
  klare, detaillierte und transparente Regelung der Arbeitsabläufe in schriftlicher Form; Unterlagen und Abläufe sind nachvollziehbar zu dokumentieren;

- Kontrollautomatik und Vier-Augen-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 Informationen an Management und Mitarbeiterinnen/Mitarbeiter, 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 (Schadensausmaß und Eintrittswahrscheinlichkeit) stehen.

Die IKS-Prinzipien werden mit Bedacht auf (im Sinne der Erreichung der Organisations- bzw. Universitätsziele) zweckmäßige, der geprüften Stelle adäquate Abläufe angewendet. Die Prinzipien der Funktionstrennung und das Vier-Augen-Prinzip sollen nicht dazu führen, dass Verantwortungen unzweckmäßig zerstückelt werden.

Die Prinzipien der Mindestinformation und der minimalen Rechte sind in erster Linie für Fragen des Zugriffs auf sensible/vertrauliche Daten für IT-Administrationsrechte und Buchungsberechtigungen relevant.

2. Begriffsdefinitionen

Risiko

Ein Risiko ist die Möglichkeit eines Schadens oder Verlustes, als Konsequenz eines bestimmten Verhaltens oder Geschehens, die die MUI an der Erfüllung ihrer Ziele und Vorhaben hindern kann.

Es wird unterschieden zwischen

- prozessbezogenen Risiken, die klar mit dem betreffenden Prozess und/oder mit einzelnen Schritten im Prozess im Zusammenhang stehen und durch Kontrollschritte minimiert werden sollen, und
- übergeordneten Risiken, die potentiell erhebliche Auswirkungen auf die Gesamtorganisation haben, ohne dabei zwingend mit einzelnen Prozessen in einem direkten Zusammenhang zu stehen.

Kontrolle

Unter Kontrollen sind Überprüfungen zu verstehen, bei welchen Inhalte mit Referenzvorgaben abgeglichen werden, um festzustellen, ob diese übereinstimmen (Soll-Ist Vergleich), einschließlich der Analyse allfälliger Abweichungen. Interne Kontrollen sind solche, die in die Prozessabläufe integriert sind.

Maßnahme

Unter der Voraussetzung, dass Abweichungen zwischen Soll und Ist bestehen oder Kontrollschwächen auftreten, denen ein Risiko innewohnt, dessen Risikograd auch nach der Berücksichtigung der Kontrolle weiterhin „sehr hoch“ oder „hoch“ ist, sind Maßnahmen zur Behebung zu definieren und umzusetzen. Dabei ist wiederum zwischen prozessintegrierten oder prozessunabhängigen steuernden Maßnahmen zur Bewältigung dieser Risiken zu unterscheiden.

3. Aufbauorganisation IKS

3.1. IKS-Verantwortung

Die Sicherstellung der IKS-Funktionsfähigkeit ist eine klare, nicht übertragbare Aufgabe der Führungsebene. Die Führungsebenen haben Vorbildwirkung bei der Einhaltung der IKS-Regeln und Vorgaben. Die Verantwortung für ein funktionsfähiges IKS an der Medizinischen Universität Innsbruck trägt das Rektorat. D.h. für die Implementierung, die laufende Anpassung und Weiterentwicklung des IKS ist das Rektorat verantwortlich.

3.2. IKS-Beauftragte/IKS-Beauftragter

Die Funktion der/des IKS-Beauftragten wird von einer Mitarbeiterin/einem Mitarbeiter der MUI wahrgenommen.

Die/Der IKS-Beauftragte hat folgende Aufgaben:

- Unterstützung der Prozessverantwortlichen bei der Implementierung und Umsetzung der Maßnahmen des IKS-Berichts
- Aufrechterhaltung und Weiterentwicklung des IKS
- Unterstützung der Internen Revision bei der Auswertung der Risiko-Kontroll-Matrix
- Erstellung des IKS-Berichtes

4. Ablauforganisation IKS

Die durch ein IKS sicherzustellenden Ziele sind:

- Sicherstellung der Unternehmenszielerreichung (Vermeidung/Verminderung externer/ interner Risiken)
- Sicherstellung IKS-gemäßer Prozesse (ordnungsgemäß, ethisch, wirtschaftlich, effizient und wirksam)
- Einhaltung der Gesetze und Vorschriften („Compliance“)
- Erfüllung der Dokumentation und Berichterstattungen

Sämtliche Prozesse werden einer Risikoanalyse unterzogen und beurteilt. Zur Vermeidung oder Minimierung der Risiken werden Kontrollaktivitäten definiert, die somit eine bestmögliche Erreichung der IKS-Unternehmensziele garantieren.

4.1. Risikobeurteilung

Für die Beurteilung der Risiken werden die Eintrittswahrscheinlichkeit (fast nie bis häufig) und das Schadensausmaß (unwesentlich bis massiv) ermittelt und dokumentiert. Dabei werden Kriterien herangezogen, die eine Gewichtung von 1-5 zulassen. Um die Risiken zu kategorisieren und zueinander in Relation zu setzen, werden das Schadensausmaß und die Eintrittswahrscheinlichkeit multipliziert. Das Schema zur Risikobeurteilung findet sich in Beilage 1.

4.2. Kontrollaktivitäten

Das IKS sieht unterschiedliche Kontrollaktivitäten vor:

Präventive Kontrollen dienen der Verhinderung des Auftretens eines Fehlers oder Unterlassungen wie z. B. Funktionstrennungen, Unterschriftenregelungen, Vier-Augen-Prinzip, klar definierte Kontrollabschnitte, die für relevante und risikogeeignete Maßnahmen gewährleisten, dass Entscheidung, Ausführung und Kontrolle nicht ausschließlich in der Hand von einer Person liegen.

Nachträgliche Kontrollen dienen der laufenden Überprüfung einer Einhaltung der IKS Vorgaben und Regelungen (z. B. Inventuren und Vollständigkeitskontrollen…).

Die MUI ist bestrebt, den Anteil an automatisierten Kontrollen soweit als möglich zu erhöhen.

Die Kombination beider Kontrollarten gewährleistet eine solide Risikosteuerung.

4.3. Maßnahmen

Maßnahmen infolge laufender Kontrollen bzw. aus dem IKS-Bericht werden entweder individuell von den Prozessverantwortlichen festgelegt und umgesetzt oder in Abstimmung mit dem/der MitarbeiterIn die/der die Kontrolle durchführte (Interne Revision).

4.4. Risiko-Kontroll-Matrix

Als Überblick und zwecks Dokumentation vor allem der mitarbeiterbedingten IKS-Kontrollen wird eine Risiko-Kontroll-Matrix (Beilage 2) erstellt. Diese bildet als Tabelle die Grundlage für die Darstellung von Kontrollinformationen iVm Risiken als auch Maßnahmen. Die Risiko-Kontroll-Matrix gilt als Grundlage eines IKS und dient als Übersicht für die Analyse und Beurteilung der prozessbezogenen Kontrollen und Maßnahmen.

5. IKS-relevante Prozesse

Die für die Hauptprozesse standardisierten Abläufe und klaren Verantwortungen werden in Prozessbeschreibungen definiert. Im Rahmen des IKS stehen besonders jene Prozesse im Fokus, welche ein hohes Risiko verbunden mit einer hohen Eintrittswahrscheinlichkeit und hohem Schadensausmaß oder ein hohes Fehler- und Betrugspotential aufweisen. Daher werden insbesondere Prozesse folgender Bereiche als IKS-relevant erachtet.

5.1. Beschaffung

Zu den IKS-relevanten Prozessen/Richtlinien der Kategorie „Beschaffung“ zählen Abläufe im Zusammenhang mit der rechtskonformen Beschaffung von Investitions-, Sach- und IT-Gütern sowie Dienstleistungen.

5.2. Finanzen

Die Kategorie Finanzen umfasst IKS-relevante Prozesse/Richtlinien aus den Bereichen Planung und Budgetierung, Berichtswesen (Monats-, Quartals- und Jahresabschluss), Steuerung/Controlling, Buchhaltung, Veranlagung, Inventarverwaltung.

5.3. Drittmittel

Unter die Kategorie Drittmittel fallen jene IKS-relevanten Prozesse/Richtlinien, welche die rechtskonforme und kaufmännisch korrekte Durchführung von Drittmittelaktivitäten gemäß geltender Richtlinie – von der Beantragung über die Durchführung bis zum Projektabschluss – gewährleisten.

5.4. IT-Nutzung

Zur IT-Nutzung zählen jene IKS-relevanten Prozesse/Richtlinien, die die Ordnungsmäßigkeit und Sicherheit der IT-Systeme gewährleisten und die Verarbeitung aller relevanten Informationen sicherstellen u.a. die Prozesse zur Vergabe von Rollen und Berechtigungen oder Richtlinien zur IT Sicherheit.

5.5. Personaladministration und Reisen

Zu den IKS-relevanten Prozessen/Richtlinien der Kategorie Personal zählen Abläufe des Personalmanagements und der Personaladministration – vom Eintritt bis zum Austritt von MitarbeiterInnen einschließlich Gehaltsabrechnung, Reisemanagement und Stammdatenpflege.

5.6. Beteiligungen

Die IKS-relevanten Prozesse/Richtlinien betreffend Beteiligungen umfassen Abläufe im Zusammenhang mit Beteiligungen und Spin offs unter Berücksichtigung der rechtlichen und wirtschaftlichen Aspekte.

6. IKS-Dokumentation der Prozesse

Um das Handeln nachvollziehbar und überprüfbar zu machen erfolgt eine Dokumentation der Prozesse und Kontrollen - die IKS-Dokumentation der unter Punkt 5 beschriebenen „finanzrelevanten“ Prozesse bildet das Kernstück des gegenständlichen Leitfadens. Diese Prozesse (Mindeststandard: Beschaffung, Finanzen, Drittmittel, IT-Nutzung, Personaladministration) sollten wie folgt dokumentiert sein:

1. Richtlinien und/oder Prozessdarstellung sowie
2. Risiko/Kontrollmatrix

6.1. Richtlinien und/oder Prozessdarstellung

Die/Der Prozessverantwortliche hat für die entsprechende Dokumentation der Prozesse als Handlungsanleitung sowie eine gesonderte Darstellung der IKS-relevanten Schritte, Kontrollen bzw. Maßnahmen Sorge zu tragen.

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

6.2. Risiko/Kontrollmatrix

Siehe dazu die Ausführungen unter Punkt 4.4.

7. Ablage der IKS-Dokumentation

Die IKS-Dokumentation erfolgt auf Basis des gegenständlichen IKS-Leitfadens. Die/Der Prozessverantwortliche ist auch für die entsprechende Ablage der Prozessdokumentation und IKS-Kontrollen bzw. IKS-Maßnahmen verantwortlich.

8. IKS-Kontroll-Überprüfung

Die Prozesse einschließlich Risiken, internen Kontrollen und Maßnahmen werden laufend von den Prozessverantwortlichen evaluiert und gegebenenfalls adaptiert.

Die Interne Revision führt periodisch und prozessunabhängig Überprüfungen der (internen) IKS-kontrollen bzw. des IKS durch. Die Ergebnisse werden in Form eines IKS-Berichtes dem Rektorat dargelegt.

9. Berichterstattung

Die Risiko- und Prozessverantwortlichen, die Risiko- und ProzesseignerInnen sowie die Kontrollverantwortlichen haben im Fall von Änderungen von IKS-relevanten Prozessschritten und (IKS-) relevanten Risiken, internen Kontrollen oder Maßnahmen die Prozesse entsprechend anzupassen und diese Änderungen an die/den IKS-Verantwortliche/n zu berichten. Es erfolgt sodann eine Berichterstattung an das Rektorat.

10. Freigabe und Inkrafttreten

Der Leitfaden wird vom Rektorat beschlossen.

Beilage 1: Risikobeurteilung

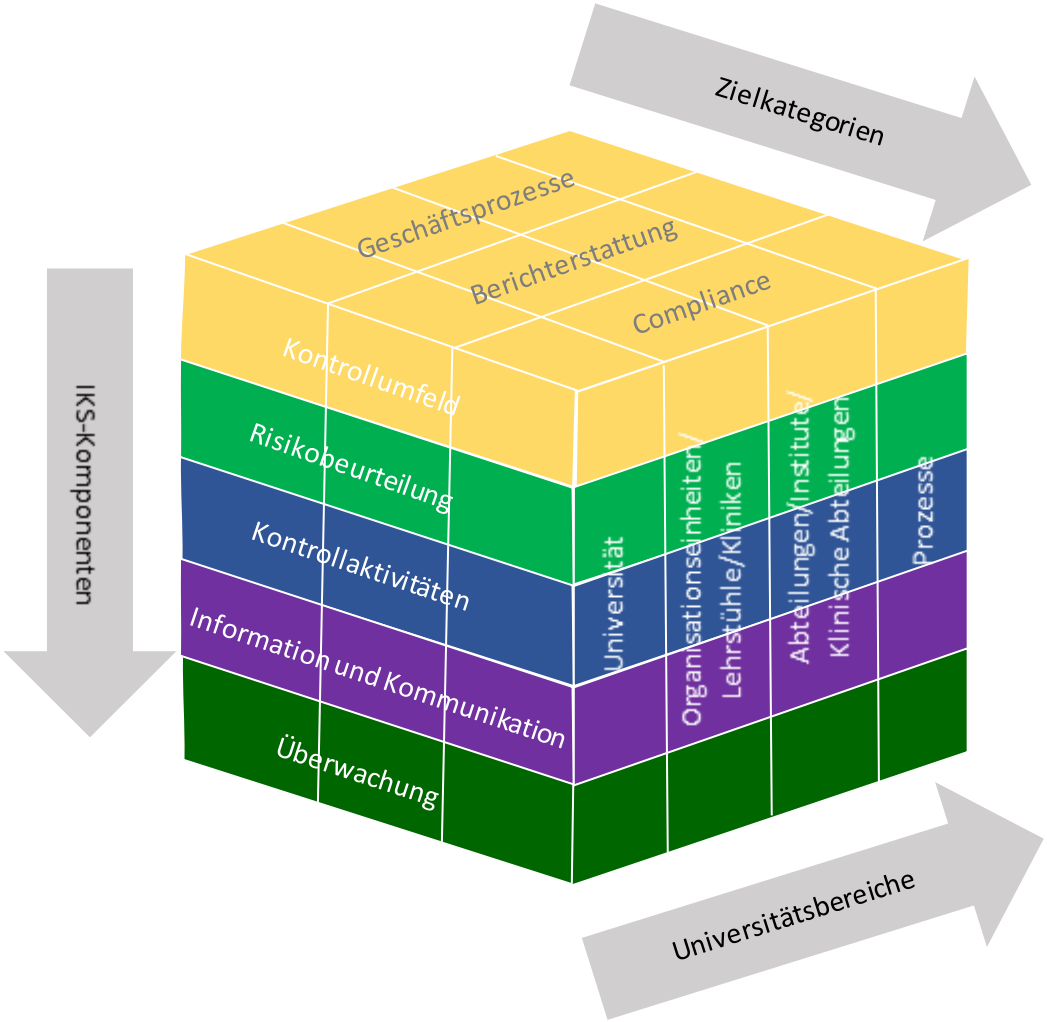
Eintrittswahrscheinlichkeit	Einstufung	Schadensereignis…	Schadens-ereignis tritt ein…	Eintrittswahr-scheinlichkeit
	1 - fast nie	kommt fast nie vor	einmal alle 10 Jahre oder mehr	≤ 1%
	2 - selten	kommt äußerst selten vor	einmal alle 5 - 10 Jahre	>1 bis ≤ 10%
	3 - gelegentlich	könnte vereinzelt eintreten	einmal alle 2 - 5 Jahre	>10 bis ≤ 20%
	4 - öfters	könnte mehrmals eintreten	Jährlich	>20 bis ≤ 50%
	5 - häufig	ist bereits vorgekommen und/oder könnte sich wiederholen	mehrmals jährlich	>50 bis <100%

Schadensausmaß	Einstufung	Gesundheitliche Auswirkung	Auswirkungen auf die Reputation der MUI	Auswirkungen auf die Aufgabenerfüllung der MUI	Finanzielle Auswirkung
	1 - unwesentlich	geringer Schaden keine Dauerfolgen	Regional leicht reversibel	geringe Beeinträchtigung einer Organisationseinheit (OE)	bis 100.000 €
	2 - niedrig	mittlerer Schaden keine Dauerfolgen	Regional reversibel	mittlere Beeinträchtigung einer OE geringe Beeinträchtigung mehrerer OEs	über 100.000 € bis 500.000 €
	3 - moderat	schwerer Schaden keine Dauerfolgen	Regional negativ kurzfristig	große Beeinträchtigung einer OE mittlere Beeinträchtigung mehrerer OEs	über 500.000 € bis 1.000.000 €
	4 - beträchtlich	schwerer Schaden mit Dauerfolgen	National negativ kurz- bis mittelfristig	hohe kurzfristige Beeinträchtigung einer oder mehrerer OEs	über 1.000.000 € bis 5.000.000 €
	5 - massiv	schwerer dauerhafter Schaden mit Lebensgefahr für Personen	National negativ langfristig International negativ kurz- bis langfristig	hohe langanhaltende Beeinträchtigung einer oder mehrerer OEs	über 5.000.000 €

Beilage 2: Risiko-Kontroll-Matrix

	Risikobeurteilung I - OHNE Berücksichtigung der Risikominimierungsmaßnahmen				Risikoverminderung		Risikobeurteilung II - MIT Berücksichtigung der Risikominimierungsmaßnahmen				Eruierung der Folgen
Risikoidentifikation	Risikobeurteilung (Auswirkung OHNE Gegenmaßnahme(n))					bereits umgesetzte Risikominimierungsmaßnahmen	Nettorisikowert (Auswirkung NACH Gegenmaßnahme(n))				Imageverlust der MUI
Risikobeschreibung (Definition)	Eintritts-wahr-schein-lichkeit / Häufigkeit (1 - 5) BRUTTO	Schadens-ausmaß / Bedeutung (1 - 5) BRUTTO	Risikowert BRUTTO (Risikoprioritäts-zahl (EW x SA)) wird berechnet	Risiko-klassifizierung (Bruttowert) wird berechnet	Ist das Risiko vermeid-, verminder- und/oder überwälzbar? ja/nein	Bereits vorhandene bzw. ergriffene Risikominimierungs-maßnahmen (Beispiele)	Eintritts-wahr-schein-lichkeit / Häufigkeit (1 - 5) NETTO	Schadens-ausmaß / Bedeutung (1 - 5) NETTO	Risikowert NETTO (Risikoprioritäts-zahl (EW x SA)) wird berechnet	Risiko-klassifizierung (Nettowert) wird berechnet	Verursacht Schadenseintritt einen Imageverlust? ja/nein/teilweise

Beilage 3: COSO-Modell



Das COSO Modell wird - wie unter Punkt 1.2. beschrieben – konkret auf die Erfordernisse bzw. Rahmenbedingungen der MUI angepasst.

Die Gliederung erfolgt in Zielkategorien, IKS-Komponenten und Universitätsbereiche.

Die 5 Komponenten (Kontrollumfeld, Risikobeurteilung, Kontrollaktivitäten, Information und Kommunikation, Überwachung) stehen zueinander in wechselseitiger Beziehung und sind in jeder der 3 Zielkategorien (Geschäftsprozesse, Berichterstattung, Compliance) zu beachten. Das IKS ist sowohl für die gesamte Universität als auch für die einzelnen Organisationseinheiten und Prozesse gültig.

Mit dem Framework 2013 wurden den fünf Komponenten des COSO– Modells insgesamt 17 Prinzipien effektiver Kontrolle zugeordnet; mit diesen Prinzipien werden die Komponenten näher ausgeführt, sie machen das Modell damit verständlicher und besser anwendbar:

COSO-Prinzipien effektiver Kontrolle (Stand 2013):

Kontrollumfeld	1. **Verpflichtung zu Integrität und ethischen Werten** – Die Organisation bekennt sich zu Integrität und ethischen Werten. 2. **Ausübung der Aufsichtspflichten** – Das Überwachungsorgan (der Universitätsrat) ist unabhängig vom Management und überwacht die Entwicklung und Funktionsfähigkeit der internen Kontrollen. 3. **Etablierung von Strukturen, Befugnissen und Verantwortlichkeiten** – Das Management (Rektorat) etabliert unter der Aufsicht des Überwachungsorgans – Strukturen, Berichtslinien sowie angemessene Befugnisse und Verantwortlichkeiten zur Verfolgung der universitären Zielkategorien. 4. **Bekenntnis zu Kompetenz** – Die Organisation demonstriert ein Bekenntnis zur Einstellung, Entwicklung und Bindung von kompetenten Personen in Übereinstimmung mit den universitären Zielen. 5. **Durchsetzung der Rechenschaft** – Die Organisation überträgt Individuen die Rechenschaftspflicht für ihre internen Kontrollen zur Verfolgung der Ziele.
Risikobeurteilung	6. **Spezifizierung von angemessenen Unternehmenszielen** – Die Organisation beschreibt zur Identifikation und Beurteilung damit verbundener Risiken die jeweiligen Ziele 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 Fraud-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.
Kontrollaktivitäten	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.
Information und Kommunikation	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.
Überwachungsaktivitäten	16. **Durchführung laufender und / oder gesonderter 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.

Vgl. *Bungartz*, Handbuch Interne Kontrollsysteme (IKS)[4] (2014) 82ff