Richtlinie des Rektorates für das interne Kontrollsystem

Montanuniversität
Leoben

Inhaltsverzeichnis

1 Ziel dieser Richtlinie 2
2 Einführung 2
2.1 Zielsetzung des Internen Kontrollsystems 2
2.2 Definition des IKS 2
2.3 Prinzipien des IKS 3
2.4 Regulatorische Anforderungen 3
2.5 Relevante Rahmenwerke 4
2.5.1 COSO – Interne Kontrollsysteme 4
2.5.2 INTOSAI GOV 9100 4
2.5.3 Das Drei-Linien-Modell des IIA (Institute of Internal Auditors) 4
2.6 Implementierung dieser Richtlinie 4
3 Verantwortlichkeiten und Rollen 5
3.1 Rektorat 5
3.2 IKS-Manager:in 5
3.3 Prozessverantwortliche 5
4 Prozess des IKS 6
4.1 Identifikation IKS-relevante Prozesse 6
4.2 Identifikation der relevanten prozessbezogenen Risiken 7
4.3 Festlegung und Definition der wesentlichen internen Kontrollen 7
4.4 Durchführung und Dokumentation des Internen Kontrollsystems 8
5 Überwachung des IKS 8
5.1 Design-Evaluierung 8
5.2 Testing 9
5.3 Umgang mit identifizierten Kontrollschwächen 10
6 IKS-Berichterstattung 11
7 Abgrenzung des IKS zu relevanten Prozessen 11
7.1 Abgrenzung zum Strategiefindungsprozess 11
7.2 Abgrenzung zur Universitätsplanung und Investitionsplanung 12
7.3 Abgrenzung zum Risikomanagement 12
7.4 Abgrenzung zur Internen Revision 12
8 Umsetzung 13
9 Inkrafttreten 13
10 Änderungsverzeichnis 13
11 Abkürzungsverzeichnis 13
12 Appendix 13

1 Ziel dieser Richtlinie

Diese Richtlinie regelt die Grundlagen für die Gestaltung des Internen Kontrollsystems (IKS) der Montanuniversität Leoben (MUL). Um die wesentlichen prozessualen Risiken im Zuge der laufenden operativen Tätigkeit in ausreichendem Maße zu adressieren, betreibt die MUL ein IKS. Das IKS der MUL hat das Ziel, prozessuale Risiken und Fehler zu erfassen sowie durch geeignete Maßnahmen zu minimieren und effiziente, einheitliche Prozessabläufe sicherzustellen.

Die nachfolgende Richtlinie bildet dabei das detaillierte Rahmenwerk zum IKS der MUL und regelt den inhaltlichen Rahmen, qualitative Mindeststandards, sowie Kompetenzen und Verantwortlichkeiten und gewährleistet, dass eine einheitliche und systematische Methode angewendet wird. Dabei wird sichergestellt, dass sich das IKS der MUL stetig weiterentwickelt und die Ziele im Rahmen der Erfüllung ihrer Aufgabenstellung erreicht.

2 Einführung

2.1 Zielsetzung des Internen Kontrollsystems

Die Grundsätze, Mindestanforderungen und Ziele des IKS sind:

- die Sicherstellung ordnungsgemäßer, ethischer, wirtschaftlicher, effizienter und wirksamer universitärer Prozessabläufe
- die unmittelbare oder mittelbare Integration der Kontroll- und Überwachungsmaßnahmen in allen wesentlichen zu überwachenden Prozessen
- die Sicherstellung der Einhaltung der Gesetze und Vorschriften sowie der implementierten Richtlinien und Verfahren
- die verlässliche Offenlegung von internen und externen finanziellen und nicht-finanziellen Informationen
- die Sicherung und Schutz des universitären Betriebsvermögens, Vermögenswerten und Ressourcen gegen Verlust, Missbrauch und Schaden
- die Sicherheit und Effizienz in der Führung der Universität durch Vermeidung von Versehen, Fehlern, aber auch dolosen Handlungen
- die Vermeidung des Gebrauchs der Universität und ihrer Mittel für unberechtigte persönliche Vorteile

2.2 Definition des IKS

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

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

2.3 Prinzipien des IKS

Im Rahmen der Umsetzung des IKS orientiert sich die MUL an den folgenden Prinzipien:

Proportionalitätsprinzip:
Die Governance-Strukturen und das IKS der MUL sind risikoorientiert und proportional zum universitären Organisationsmodell auszugestalten. Entwicklung und Umsetzung haben Größe, interne Organisation, sowie Art, Umfang und Komplexität der Organisationstätigkeit angemessen zu berücksichtigen.

Wirtschaftlichkeit:
Das IKS der MUL orientiert sich am Grundsatz der Wirtschaftlichkeit, Rechtmäßigkeit und Zweckmäßigkeit in Bezug auf die getroffenen Organisationsregelungen und den zu ergreifenden Kontrollmaßnahmen.

Funktionstrennung:
Die Funktionstrennung ist ein Konzept zur Trennung von Aufgaben, die aus Sicht des Risikomanagements unvereinbar sind. Mit Hilfe der Funktionstrennung soll sichergestellt werden, dass keine einzelne Person die Kontrolle über zwei oder mehrere in Konflikt stehende Aufgaben hat. Die Funktionstrennung muss sowohl organisatorisch als auch systemisch gewährleistet sein.

Offenheit:
Mangelhafte Kontrollen hinsichtlich des Designs und der Effektivität sind rechtzeitig, richtig und vollständig an die verantwortlichen Entscheidungsträger zu kommunizieren.

Transparenz:
Prozesse werden klar, einheitlich und nachvollziehbar dokumentiert. Prozessbezogene Risiken, die entsprechenden Kontrollen sowie die Nachweise der Kontrolldurchführung müssen nachvollziehbar dokumentiert, aufbewahrt und auf Verlangen bereitgestellt werden.

Regelmäßige Evaluierung:
Unabhängige regelmäßige Überprüfungen des IKS auf Effektivität, Nachhaltigkeit und Funktionsfähigkeit tragen zur Zuverlässigkeit und Effizienz der Abläufe bei.

2.4 Regulatorische Anforderungen

Rechtliche Grundlagen für das IKS der MUL bilden im Wesentlichen:
Universitätsgesetz - § 15 Abs. 1 UG:

- Die Gebarung der Universität ist nach den Grundsätzen der Rechtmäßigkeit, Wirtschaftlichkeit, Zweckmäßigkeit, Sparsamkeit und Transparenz zu gestalten.
- Der Haushalt der Universität ist mit entsprechender Sorgfalt zu führen.

B-PCGK Bundes-Public Corporate Governance Kodex Regel 11.1.1.2 BPCGK:

- Die Tätigkeit des Überwachungsorgans umfasst jedenfalls die Überwachung des Risikomanagements und des internen Kontrollsystems des Unternehmens.

2.5 Relevante Rahmenwerke

2.5.1 COSO – Interne Kontrollsysteme

Das IKS der MUL orientiert sich an den Prinzipien des internationalen Rahmenwerks zu Internen Kontrollen, welches 2013 durch das Committee of Sponsoring Organizations of the Treadway Commission (COSO-Rahmenwerk) etabliert und im März 2023 überarbeitet wurde. Das COSO-Rahmenwerk stellt einen unverbindlichen Leitfaden für die Gestaltung, Implementierung und Überwachung des IKS dar.

Die Aufgaben des IKS nach COSO sind neben der Bewahrung des Vermögens, die Gewährleistung der Zuverlässigkeit des Rechnungs- und Berichtswesens, die Verbesserung der Effizienz betrieblicher Abläufe sowie Transparenz und Nachvollziehbarkeit von Abläufen zum Schutz der Prozessbeteiligten, die Einhaltung gesetzlicher und sonstiger rechtlicher Grundlagen (Compliance) und die ordnungsgemäße Geschäftsführung und Einhaltung der Geschäftspolitik.

2.5.2 INTOSAI GOV 9100

Neben COSO sind die Richtlinien des INTOSAI GOV 9100 Standards für die internen Kontrollnormen im öffentlichen Sektor ergänzend heranzuziehen. Primär richtet sich die Ausgestaltung des IKS an der MUL jedoch nach COSO. Der INTOSAI GOV 9100 Standard orientiert sich überwiegend am COSO Internal Control Framework und gibt ebenso Hilfestellung für die Ausgestaltung eines Internen Kontrollsystems. Dabei zeigt INTOSAI einen Rahmen auf, wie das IKS eingebettet und entsprechende Kontrollen aufgesetzt werden können. Das IKS wird bei INTOSAI als ein dynamisch integraler Prozess beschrieben, welcher durch das Management und die MitarbeiterInnen einer Organisation beeinflusst wird.

Das Modell in dem INTOSAI Standard besteht aus den gleichen Elementen und Komponenten wie bei COSO, wird jedoch um eine Zielkategorie erweitert („safeguarding ressources“). Damit zielt der INTOSAI Standard auf die spezifischen Anforderungen des öffentlichen Sektors ab, vor allem im Hinblick auf die Sicherung/Schutz von Vermögenswerten und ethischem Verhalten.

2.5.3 Das Drei-Linien-Modell des IIA (Institute of Internal Auditors)

Gemäß dem „Drei-Linien-Modell“ des Institute of Internal Auditors werden Risiken in drei Stufen identifiziert, überwacht und gesteuert. Das Konzept bietet einen Rahmen zur Ausgestaltung der Corporate Governance innerhalb einer Organisation, indem entsprechende Rollen und Verantwortlichkeiten definiert werden.

2.6 Implementierung dieser Richtlinie

Die vorliegende Richtlinie bildet eine verbindliche Grundlage für das IKS der MUL und richtet sich an alle Führungskräfte und Mitarbeitende der MUL, welche im Rahmen ihrer Aufgaben in das IKS eingebunden sind. Die vorliegende Richtlinie gilt unbefristet, Änderungen und Adaptionen erfolgen im Bedarfsfall.

3 Verantwortlichkeiten und Rollen

An der MUL wird ein IKS eingerichtet, das die Entscheidungsträger:innen in ihren jeweiligen Zuständigkeitsbereichen wirksam unterstützt. Die in dieser Richtlinie festgelegten Rollen und Verantwortlichkeiten im IKS sind verpflichtend umzusetzen und im täglichen Arbeitsablauf konsequent zu verankern. Die Vorgaben zum IKS sind dynamisch auszulegen und bei veränderten Rahmenbedingungen fortzuschreiben, zu ergänzen und entsprechend anzuwenden.

Für das IKS sind an der MUL nachstehende Funktionen mit klar zugewiesenen Verantwortlichkeiten und Kompetenzen ausgestattet:

3.1 Rektorat

Das Rektorat der MUL legt die Ziele und Strategien für das IKS sowie die Universitätsstandards (dargestellt in dieser Richtlinie) fest. Dabei liegt die Gesamtverantwortung für die Einrichtung und angemessene Ausgestaltung eines wirksamen IKS bei dem Rektorat. Das Rektorat überträgt die Aufgaben des IKS-Prozesses an eine/n IKS-Manager:in und genehmigt gegebenenfalls relevante Steuerungsmaßnahmen für zentrale Kontrollen.

Das Rektorat trifft Entscheidung über Aufbau- (IKS-Verantwortlichkeiten) und Ablauforganisation (Prozesse) des organisationsweiten Internen Kontrollsystems, überwacht und beurteilt regelmäßig die Wirksamkeit des IKS und verabschiedet Soll-Vorgaben.

3.2 IKS-Manager:in

Der/Die IKS-Manager:in ist für das hier beschriebene universitäre Interne Kontrollsystem verantwortlich, entwickelt die universitäre IKS-Systematik weiter und sorgt für die Aktualisierungen von Methodik und der Richtlinie. Der/Die IKS-Manager:in erstellt die Unterlagen für die IKS-Berichterstattung. Jährlich, bzw. im Bedarfsfall ad-hoc, berichtet der/die IKS-Manager:in an das Rektorat der MUL und legt dem Rektorat alle Ergebnisse der Effektivitätsüberwachung im IKS sowie die wesentlichen identifizierten Schwachstellen in den Internen Kontrollen vor. Im Bedarfsfall nimmt der/die IKS-Manager:in an der Rektoratssitzung teil, um über das Interne Kontrollsystem zu berichten. Dabei entwickelt der/die IKS-Manager:in Methoden und Vorgaben zur Weiterentwicklung des IKS. Zu den Aufgaben der/des IKS-Manager:in zählen auch die Beratung und Unterstützung der Prozessverantwortlichen. Der/Die IKS-Manager:in bildet demnach die zentrale Einheit zur Umsetzung, Weiterentwicklung, Koordination, Verwaltung, Dokumentation und Berichterstattung des IKS.

3.3 Prozessverantwortliche

Prozessverantwortliche tragen die Verantwortung für die Funktionsfähigkeit einer oder mehrerer Kontrollen in den ihnen verantworteten Prozessen. Zum Verantwortungsbereich der Prozessverantwortlichen gehören unter anderem folgende Tätigkeiten:

- **Risikoidentifikation:** Identifikation der prozessrelevanten Risiken innerhalb des Verantwortungsbereiches

- **Bewertung der Prozessrisiken:** Einschätzung, ob ein prozessbezogenes Risiko relevant ist und in die IKS-Dokumentation aufgenommen werden sollte
- **Interne Kontrollen:** Definition des geeigneten Kontrollansatzes, Implementierung geeigneter interner Kontrollen, Sicherstellung der Abdeckung des Risikos durch die identifizierten Kontrollen, Abstimmung mit Prozessverantwortlichen aus vor- und nachgelagerten Prozessen, um die entsprechende Umsetzung und Durchführung von internen Kontrollen sicherzustellen und Synergien zu nutzen, Verantwortung für die Aktualität der Prozesse und Kontrollen im verantworteten Bereich
- **IKS-Assessment:** Zumindest einmal jährlich (oder im Anlassfall) Durchführung einer Aktualisierung der Risiko- und Kontrollmatrix bezüglich Vollständigkeit und Aktualität
- **IKS-Kommunikation:** Identifikation und Dokumentation von neuen prozessbezogenen Risiken und entsprechenden Kontrollen (insbesondere bei Änderungen), Reporting der aktualisierten Risiko- und Kontrollmatrix an den/die IKS-Manager:in

4 Prozess des IKS

Der Nutzen eines IKS besteht darin, dass Risiken durch den Einsatz von Kontrollen aktiv minimiert werden können, alle maßgeblichen Vorschriften und Gesetze eingehalten werden, sowie sämtliche materielle wie immaterielle Vermögenswerte vor Verlust, Missbrauch und Schaden gesichert sind.

Im Folgenden wird, der in der MUL angewandte IKS-Prozess beschrieben.

4.1 Identifikation IKS-relevante Prozesse

Im Zuge der Identifikation der für das IKS als relevant eingestuften Prozesse folgt man an der MUL den durch das Bundesministerium veröffentlichten Empfehlungen zu den IKS-Mindeststandards für Universitäten. Demnach liegt der Fokus des IKS der MUL auf den finanzrelevanten Prozessen, welche im Zuge des IKS und zur Abdeckung der Mindestanforderungen in das IKS einzubeziehen sind.

Finanzrelevante Prozesse:

- Beschaffung
- Finanzen (Budgetierung, Berichtswesen, Steuerung, Rechnungslegung, Veranlagung, Liquiditätssicherung, Handkassa, Bankgarantien)
- Drittmittel und Fundraising
- IT-Nutzung
- Personaladministration & Reisen

Für jeden dieser finanzrelevanten Prozesse ist im Sinne der IKS-Dokumentation eine Risiko- und Kontrollmatrix (RKM) und eine Richtlinie und/oder eine Prozessdarstellung zu erstellen.

Eine Übersicht zu den Prozessen und den überblicksmäßigen Inhalten befindet sich in Anlage C Prozessübersicht.

4.2 Identifikation der relevanten prozessbezogenen Risiken

Es liegt in der Verantwortung des Prozessverantwortlichen die relevanten inhärenten Prozessrisiken zu identifizieren, zu definieren und gemäß einheitlicher Vorgangsweise zu dokumentieren und zu adressieren.

Ein inhärentes Risiko ist ein Risiko, welches eine grundsätzliche Wahrscheinlichkeit des Auftretens hat, ohne Betrachtung von mitigierenden (das Risiko minimierenden) Kontrollen. Dies bedeutet, dass es das jeweilige Risiko grundsätzlich im zugrundeliegenden Prozess gibt, unabhängig davon, ob das Risiko durch geeignete Kontrollen adressiert/vermindert wird oder nicht.

4.3 Festlegung und Definition der wesentlichen internen Kontrollen

Interne Kontrollen sollen sicherstellen, dass wesentliche prozessbezogene Risiken im Rahmen der operativen Tätigkeit aufgedeckt oder präventiv verhindert werden. Dabei werden bestehende Risiken erfasst, gesteuert und sichergestellt, dass die betroffene Organisation, im Rahmen der Erfüllung ihrer Aufgabenstellung, ihre Ziele erreicht.

Die Festlegung und Definition der relevanten internen Kontrollaktivitäten obliegt den zuständigen Prozessverantwortlichen der MUL. Zielsetzung ist, dass für alle identifizierten, relevanten, prozessbezogenen Risiken entsprechende Kontrollen implementiert sind, welche das identifizierte Risiko adressieren und abdecken. Bei identifizierten Kontrollschwächen sind die entsprechenden Maßnahmen seitens der Prozessverantwortlichen einzuleiten.

Für jeden als für das IKS als wesentlichen einzustufenden Prozess ist eine RKM (Risiko- und Kontrollmatrix) (Template siehe Anlage A) zu erarbeiten und durch den Prozessverantwortlichen aktuell zu halten (anlassbezogen bzw. mindestens jährliches Assessment).

Eine RKM ist ein Werkzeug, welches dazu verwendet wird, Risiken mit den dazugehörigen Schlüsselkontrollen zu verlinken und ein bestehendes IKS nachvollziehbar dokumentieren zu können.

In die RKM sind nur als wesentlich einzustufende Schlüsselkontrollen aufzunehmen. Ziel ist es nicht, sämtliche Kontrollen, die in den unterschiedlichsten Prozessen durchgeführt werden, aufzunehmen, sondern sich auf die wesentlichen Kontrollpunkte zu konzentrieren.

Die Einstufung einer Kontrolle als Schlüsselkontrolle obliegt dem jeweiligen Prozessverantwortlichen auf Basis seiner persönlichen Einschätzung, Fachkompetenz und Erfahrung je Kontrolle.

Grundsätzlich sind als Schlüsselkontrollen jene Kontrollen zu verstehen, welche für sich genommen oder in Verbindung mit anderen Kontrollen, ein oder mehrere signifikante/wesentliche Risiken adressiert und bei welchen sich das Management darauf verlässt, dass sie eine angemessene Sicherheit darüber geben, dass nur ein geringfügiges Restrisiko darüber besteht, dass das Risiko eintritt.

Schlüsselkontrollen decken für gewöhnlich das größte finanzielle Risiko ab und decken die Frage nach „was könnte schiefgehen“ bestmöglich ab.

4.4 Durchführung und Dokumentation des Internen Kontrollsystems

Die definierten Kontrolldurchführenden sind für die regelmäßige Durchführung der ihnen verantworteten Kontrollen und deren Dokumentation verantwortlich. Kontrollen sind in Übereinstimmung mit den definierten Kontrollaktivitäten laut RKM durchzuführen und zu dokumentieren (Erstellung eines Kontrollnachweises). Es gilt der Grundsatz: „was nicht dokumentiert ist, wurde nicht durchgeführt“.

Die Kontrolldokumentation muss:

- nachvollziehbar (also derart beschaffen sein, dass sie von einem sachverständigen Dritten innerhalb angemessener Zeit verstanden werden kann),
- vollständig (der/die Geschäftsvorfall/Kontrollaktivität muss sich in seiner Entstehung und Abwicklung verfolgen lassen),
- verständlich (die Aufzeichnungen müssen in einer lebenden Sprache geführt werden)
- richtig, zeitgerecht und strukturiert und
- unveränderbar (Aufzeichnungen dürfen nicht derart verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist und es muss auch Klarheit darüber bestehen, wann und durch wen die Aufzeichnung erstellt wurde) sein.

Eine IKS-Dokumentation in elektronischer Form ist möglich und bevorzugt.

Die Aufbewahrungspflicht für die IKS-Dokumentation (v.a. Kontrollnachweise) richtet sich nach dem UGB und wird mit sieben Jahren festgelegt. In diesem Zeitraum muss es jederzeit möglich sein die angefragte Kontrolldokumentation vorzeigen zu können.

Für jeden Prozessbereich sind die erforderlichen Mindestanforderungen und die jeweilige prozessspezifische IKS-Dokumentation - Richtlinie und/oder Prozessbeschreibungen, sowie die Risiko- und Kontrollmatrix – lokal abzulegen und auf Verlangen vorzulegen.

5 Überwachung des IKS

5.1 Design-Evaluierung

Durch die Prozessverantwortlichen ist einmal jährlich nach Vorgabe des Zeitplans durch den/die IKS-Manager:in, eine Aktualisierung der RKM durchzuführen. In diesem Zusammenhang sind die Risiken sowie die zugehörigen Kontrollen u.a. auf Vollständigkeit und Aktualität hin zu überprüfen und ggfs. anzupassen.

Nach erfolgter Evaluierung, Analyse und Aktualisierung hat der Prozessverantwortliche die aktualisierte RKM an den den/die IKS-Manager:in zu übermitteln.

5.2 Testing

Um die Wirksamkeit der festgelegten Kontrollen nachzuweisen, ist mit Hilfe periodischer Tests die ordnungsgemäße Durchführung der definierten Kontrollen zu überprüfen. Unter einem IKS-Testing wird eine Testung der Kontrollen auf Stichprobenbasis verstanden, um festzustellen, ob die Kontrollen, wie in der RKM beschrieben, in der laufenden operativen Tätigkeit auch adäquat durchgeführt werden.

Als Tester fungiert die Interne Revision, die unter Einhaltung der Vorgabe der Unabhängigkeit das Testing durchführen.

Das IKS-Testing muss durch die Interne Revision derart ausgestaltet sein, dass in einem Zeitraum von drei Jahren alle Kontrollen eines Prozessbereichs zumindest einmal einem IKS-Testing unterzogen werden und jedes Jahr zumindest ein Teil der Kontrollen eines Prozessbereichs getestet wird.

Des Weiteren ist ein IKS-Testing im Bedarfsfall ad-hoc oder häufiger durchzuführen, wenn sich nach Einschätzung der Prozessverantwortlichen oder des/der IKS-Manager:in ein (risikoorientierter) Anlassfall ergibt. Indikatoren für eine höhere Testfrequenz können u.a. sein:

- Fall eines ad-hoc Risikos
- Änderungen im Prozess oder bei einer Kontrolle
- Unregelmäßigkeiten
- mangelndes Kontrollbewusstsein
- neue Geschäftsfelder bzw. Umstrukturierung des Unternehmens
- Veränderung in der IT-Landschaft
- personelle Veränderungen (Personalfluktuation, Generationenwechsel)
- Häufungen von atypischen Geschäftsabläufen bzw. –fällen
- schwerwiegende Beanstandungen bei früheren IKS-Prüfungen

Im Zuge des stichprobenbasierten IKS-Testing ist sowohl das Design der Kontrolle (konzeptionelle Wirksamkeit) als auch die operative Wirksamkeit zu beurteilen. Die Testinghandlungen und deren Ergebnisse sind in einem einheitlich zu verwendenden IKS-Testingprotokoll (Template siehe Anlage B) zu dokumentieren.

Der Umfang der zu ziehenden jährlichen Stichproben richtet sich nach der Kontrollfrequenz der jeweils zu testenden Schlüsselkontrolle (Jahresbetrachtung).

Kontrollfrequenz	Stichprobengröße
Mehrmals täglich	10
Täglich	10
Wöchentlich	4
Monatlich	3
Quartalsweise	2
Halbjährlich	2
Jährlich	1
Anlassbezogen	10% der Transaktionen, max. 10
Automatisierte Kontrollen	1

Die erfolgten Testing-Aktivitäten sind in einem standardisierten Testing-Protokoll festzuhalten und zu dokumentieren. Die gesamte Testing-Dokumentation (Testing-Protokoll und alle Arbeitspapiere (wie zB Stichproben, Stichprobenziehung, Auswertung der Stichproben) sind aufzubewahren und auf Verlangen vorzuweisen.

Testing-Aktivitäten sind einmal jährlich vor einer Uniratssitzung durchzuführen. Der konkrete Zeitplan wird durch die Interne Revision definiert.

5.3 Umgang mit identifizierten Kontrollschwächen

Auf der Grundlage der Testergebnisse werden die getesteten internen Kontrollen entweder als wirksam oder als unwirksam eingestuft. Im Falle wirksamer Kontrollen (sowohl konzeptuelle als auch operative Wirksamkeit) werden die Strukturen und Prozesse der Internen Kontrolle beibehalten und gegebenenfalls weitere Effizienzsteigerungen der Kontrollen initiiert und umgesetzt.

Interne Kontrollen gelten als unwirksam, wenn sich herausstellt, dass die Erreichung entsprechender Kontrollziele nicht sichergestellt werden kann, und/oder wenn die internen Kontrollen nicht wirksam funktionieren.

Sobald eine getestete Interne Kontrolle als "unwirksam" eingestuft wurde, sind entsprechende Maßnahmen zu definieren, welche darauf abzielen, festgestellte Mängel in der Kontrollgestaltung und/oder der operativen Wirksamkeit zu beheben. Die Kontrollverantwortlichen sind für die Definition und Umsetzung von Maßnahmen zur Heilung des identifizierten Kontrollmangels und zur Erreichung des definierten Kontrollziels

verantwortlich. Zwischen Interner Revision und Kontrollverantwortlichen ist ein Zeitplan zur Umsetzung abzustimmen. Nach erfolgter Umsetzung werden die Tests wiederholt, um das Design und/oder die operative Wirksamkeit der überarbeiteten Internen Kontrolle zu beurteilen. Das erneute Testen ist innerhalb eines angemessenen Zeitrahmens erforderlich.

6 IKS-Berichterstattung

Um das Risikobewusstsein zu fördern ist eine aufrechte Kommunikation erforderlich. Ein IKS muss im Rahmen der Aufgabe einer Risikokommunikation verschiedene Adressatenkreise mit den relevanten Informationen versorgen. Der/Die IKS-Manager:in der MUL berichtet über den Status des IKS an das Rektorat.

Der IKS-Bericht umfasst folgende Inhalte:

- Management Summary
- Zusammenfassende, qualitative Einschätzung der Wirksamkeit des IKS in der Organisation
- Beschreibung und Darstellung der aktuellen IKS-Struktur sowie etwaiger Änderungen gegenüber dem Vorjahr (Verantwortlichkeiten und Rollen)
- Zusammenfassender Gesamtüberblick der Ergebnisse des IKS-Testings mit Vorperiodenvergleich
- Detaillierte Informationen zum Ergebnis des IKS-Testings pro Prozess
- Zusammenfassung der wichtigsten Themen (Effektivität, größte Risiken, Ausblick)

Die Inhalte des Berichts sind aktuell zu halten und eine vollständige und korrekte Berichterstattung zu vordefinierten Terminen ist sicherzustellen.

Für den Fall, dass ein wesentliches Risiko, das aus einer Schwachstelle des IKS entsteht, identifiziert wird, gibt es bei der MUL neben dem regulären Berichtsformat auch einen Ad-hoc-Reporting Prozess.

7 Abgrenzung des IKS zu relevanten Prozessen

Das IKS der MUL besteht aus systematisch gestalteten, aufeinander abgestimmten organisatorischen Maßnahmen, Methoden und Kontrollen zur Einhaltung interner und externer Richtlinien, zur Abwehr von Schäden und zur Erfüllung der Berichterstattungspflicht (nach UGB und Universitätsvorgaben). Das IKS soll somit sicherstellen, dass Geschäftsprozesse funktionsfähig und wirtschaftlich sind, das universitäre Vermögen gesichert ist, universitäre Informationen zuverlässig sind und Gesetze und interne Normen eingehalten werden.

7.1 Abgrenzung zum Strategiefindungsprozess

Der Strategiefindungsprozess und das integrierte Risikomanagement der MUL binden strategisch relevante Risiken und Maßnahmen systematisch in die Strategieverfolgung ein. Demgegenüber ist das IKS kein Instrument der Strategiedefinition, sondern dient der regelkonformen, effizienten und dokumentierten Umsetzung strategischer Vorgaben. Der Fokus des IKS liegt schwerpunktmäßig im operativen, prozessorientierten Bereich.

7.2 Abgrenzung zur Universitätsplanung und Investitionsplanung

Die Planung bildet den Erwartungswert für den zukünftigen Geschäftsverlauf der Universität ab. In ihr sind daher Risiken bereits enthalten, diese werden jedoch auf einen Planwert verdichtet dargestellt. Das IKS ergänzt die Planung nicht durch Risikobewertung, sondern durch die Absicherung ordnungsgemäßer, wirtschaftlicher und nachvollziehbar dokumentierter Abläufe, damit Plan- und Investitionsvorgaben regelkonform freigegeben, durchgeführt und überwacht werden.

7.3 Abgrenzung zum Risikomanagement

Ein Internes Kontrollsystem (IKS) besteht aus systematisch gestalteten, aufeinander abgestimmten, organisatorischen Maßnahmen, Methoden und Kontrollen zur Einhaltung von (internen und externen) Richtlinien, zur Abwehr von Schäden und zur Erfüllung der Berichterstattungspflicht (nach UGB und Universitätsvorgaben). Ein IKS soll somit sicherstellen, dass Geschäftsprozesse funktionsfähig und wirtschaftlich sind, das universitäre Vermögen gesichert ist, universitäre Informationen zuverlässig sind und Gesetze und interne Normen eingehalten werden.

Während sich das Risikomanagement strategisch mit der Risikosituation an der Universität auseinandersetzt und den Fokus zukunftsorientiert auf Sachverhalte legt, die das Erreichen von Ergebniszielen beeinflussen können, liegt die Betrachtungsweise des IKS schwerpunktmäßig im operativen, prozessorientierten Bereich und dient der Umsetzung der oben definierten Anforderungen. Eine im Risikomanagement festgelegte Maßnahme wird sinnvollerweise dann ins IKS überführt werden, wenn sie über einen längeren Zeitraum regelmäßig wiederkehrend durchgeführt wird, wobei die Durchführung aus Gründen der Überprüfbarkeit nachvollziehbar zu dokumentieren ist.

7.4 Abgrenzung zur Internen Revision

Die Interne Revision ist eine außerhalb der operativen universitären Prozesse angesiedelte, neutrale Stelle, die durch systematische Prüfungen die Ordnungsmäßigkeit, Funktionsfähigkeit, Sicherheit, Wirtschaftlichkeit und Rechtmäßigkeit der betrieblichen Abläufe überwacht. Das Risiko im Sinne des Internen Kontrollsystems stellt für die Universitätsrevision eine Lenkungsgröße zur Fokussierung der Prüfungstätigkeit auf riskante und damit eher fehleranfällige Abläufe, Systeme, Situationen oder Zustände. Es kann daher auch das Interne Kontrollsystem selbst, d.h. die Handhabung des IKS, zum Gegenstand der Prüfungstätigkeit werden.

Die Prozessverantwortlichen sind verantwortlich für eine kontinuierliche Kontrolle der Maßnahmen zur Risikosteuerung hinsichtlich deren Wirksamkeit. Die Universitätsrevision hat bei ihrer Prüfungstätigkeit die Handhabung, Aussagekraft und Wirksamkeit des IKS zu prüfen und zu beurteilen.

Die Interne Revision führt die Wirksamkeitsüberprüfung im IKS durch.

8 Umsetzung

Die vorliegende IKS-Richtlinie bildet eine verbindliche Grundlage für das IKS an der MUL.

9 Inkrafttreten

Diese Richtlinie tritt mit dem Ablauf des Tages ihrer Kundmachung im Mitteilungsblatt der Montanuniversität Leoben in Kraft.

10 Änderungsverzeichnis

Version	Aktivität	Ersteller	Datum
1.0	Erstversion	Finance	24.02.2026

11 Abkürzungsverzeichnis

Abkürzung	Definition
COSO	Committee of Sponsoring Organizations der Treadway Commission
IKS	Internes Kontrollsystem
MUL	Montanuniversität Leoben
RKM	Risiko- und Kontrollmatrix

12 Appendix

Anlage	Inhalt
Anlage A	Template Risiko- und Kontrollmatrix
Anlage B	Template Testingprotokoll
Anlage C	Prozessübersicht

Für das Rektorat:
Der Rektor
Univ.-Prof. Dipl.-Ing. Dr.mont. Dr.-Ing.E.h. Dr.h.c. Peter Moser

Anlage A: Risiko- und Kontrollmatrix

Risiko- und Kontrollmatrix

Hauptprozess	Subprozess	Prozessverantwortliche*r	Risikobeschreibung	Kontroll-ID	Kontrollbeschreibung	Identifiziertes GAP/ Weiterentwicklungspotential	Kontrolldurchführer*in	Kontrollnachweis	Kontrollfrequenz	Kontrolltyp	Kontrollmethode	zugrundeliegende Richtlinie

Risiko- und Kontrollmatrix - Ausfüllhilfe

Feld	Beschreibung
Hauptprozess	Nennung Hauptprozess
Subprozess	Nennung Subprozess
Prozessverantwortlicher	Nennung des Prozessverantwortlichen (jene Person welche gesamthaft den jeweiligen Prozess organisatorisch verantwortet)
Risikobeschreibung	Beschreibung des relevanten Prozess-Risikos. Fragen sie sich bei der Identifikation und Formulierung des Risikos was im jeweiligen Prozess/der jeweiligen Aktivität schief gehen könnte.
Kontroll-ID	Vergabe Kontroll-ID
Kontrollbeschreibung	Beschreibung der gesetzten Kontrollaktivität. Anhand der Kontrollbeschreibung sollten die Kontrollen von einem sachkundigen Dritten nachvollzogen werden können. Beatworten sie im Zuge der Kontrollbeschreibung die folgenden Fragestellungen: - Wer führt die Kontrollaktivität aus? - Was ist die Kontrollaktivität? - Wann wird die Kontrollaktivität ausgeführt? - Wie wird die Kontrollaktivität ausgeführt und wie wird diese dokumentiert/belegt? Im Zuge der Kontrollbeschreibung wird nur mit Funktionen und nicht mit Namen gearbeitet. Dies erleichtert die laufende Aktualisierung der RKM.
Identifiziertes GAP/ Weiterentwicklungspotential	Nennung des GAPs / Weiterentwicklungspotenzial
Kontrolldurchführer	Nennung des Kontrolldurchführer (jene Fuktion/Funktionen und Person/Personen welche die Kontrolle aktiv durchführen)
Kontrollnachweis	Nennung des Kontrollnachweis (wie wird die Kontrolle dokumentiert und belegt)
Kontrollfrequenz	Angabe der Kontrollfrequenz. Wie oft wird die Kontrolle durchgeführt. Die gewählte Kontrollfrequenz muss mit der dahinterliegenden Kontrollaktivität im Einklang stehen und sollte sicherstellen, dass die Kontrolle unter Risikogesichtspunkten ausreichend oft durchgeführt wird. Auswählbare Kontrollfrequenzen: - täglich - wöchentlich - monatlich - quartalsweise - halbjährlich - jährlich - anlassbezogen
Kontrolltyp	Angabe Kontrolltyp präventiv: vorbeugende Vermeidung von Fehlern (eine Kontrollaktivität, die verhindern soll, dass etwas schief geht, sodass ein Fehler vermieden werden kann. Die Kontrolle wird normalerweise durchgeführt, bevor Finanzzahlen erfasst werden oder der Sachverhalt realisiert wird) detektiv – nachträgliche Aufdeckung und Korrektur von Fehlern (eine Kontrollaktivität, die dazu dient, Fehler oder Unregelmäßigkeiten, rechtzeitig zu erkennen und zu korrigieren- detektive Kontrollen sind normalerweise Aktivitäten, die ausgeführt werden, nachdem eine Finanzzahl erfasst, ein IT-Zugang gewährt oder ein Sachverhalt abgeschlossen wurde)
Kontrollmethode	Angabe Kontrollmethode Manuell – manuelle Kontrolldurchführung (erfordern menschliche Eingriffe und verlassen sich nicht au automatisierte Funktionen) automatisiert – automatisierte Kontrolldurchführung durch das System ohne manuellen Eingriff IT-abhängig – Mischform aus manueller und automatisierter Kontrolle bei welcher systemgestützt manuelle Kontrollaktivitäten gesetzt werden - werden von einer Person ausgeführt, die auf automatisierte Ausgaben angewiesen ist
zugrundeliegende Richtlinie	Nennung der zugrundeliegenden Richtlinie

Testingprotokoll

Hauptprozess:	
Subprozess:	

Tester:	
Datum des Tests:	

Kontrollnummer:	
Kontrollbeschreibung:	
Kontrollmethode:	
Kontrollfrequenz:	
Stichprobengröße:	
Testperiode:	

Beurteilug Design-Effectiveness:	
Beschreibung identifizierte Schwäche des Designs:	

Test Plan

Methode des Testings	
Erhebung/Interview	
Überwachung	
Überprüfung der physischen Evidenz	
Re-Performance	
Analytisches Verfahren	

Attribut ID	**Detaillierte Test-Beschreibungen (getestete Attribute)**
A	
B	
C	
D	

Test Ergebnisse

			Ergebnis geteste Attribute					
Stichprobe No.	**Beschreibung Stichprobe**	**Datum Stichprobe**	**A**	**B**	**C**	**D**	**Schlussfolgerung pro Stichprobe**	**Referenz zu Unterlagen**

Legende für Ergebnis getestete Attribute

Legende	**Erklärung**
P	
N/A	
x	

Beurteilug Operative-Effectiveness:	
Beschreibung identifizierte Schwäche der Operative Effectiveness:	

Anlage C: IKS Prozessübersicht

IKS Prozessübersicht

Prozessbereich	Subprozess	Stichworte/Themengebiete zum Subprozess
Beschaffung	Lieferantenauswahl	Lieferantenauswahl (Kriterien), Lieferantenscreening, Einkaufsrichtlinie, Ausschreibung, Angebote (Angebotsauswahl)
	Bestellabwicklung	Erstellen und Genehmigen von Bestellungen, Bestellfreigaben, Umgang mit Bestelländerungen, Genehmigungsmatrix, Berechtige Personen für das Erstellen und Genehmigen einer Bestellung, Übermittlung von Bestellungen an den Lieferanten, Überwachung Rechnungen ohne Bestellung
	Vertragswesen	Vertragsvorlagen, Einbindung Rechtsabteilung in Lieferantenverträge, Abschuss von Verträge (Überprüfung von korrekten Vertragsbestandteilen, Zeichnung von Verträgen), Genehmigungsmatrix, Vertragsmanagement (Laufzeitenanalyse, Archivierung, Kündigung, Verlängerung)
	Wareneingang	Warenübernahme, Entgegennahme der Leistung, Wareneingangsprüfung, Wareneingangsverbuchung, Umgang mit Beanstandungen und Rücksendungen
Finanzen	Planung und Budgetierung	Kommunikation Budgetvorgaben, Erstellung Budget, Überprüfung und Genehmigung Budget, Genehmigungsmatrix, Planungsgespräche, Zusammenführung Gesamtbudget, laufende Budgetüberwachung, Umgang mit Budgetüberschreitungen
	Berichtswesen und Steuerung	Externe Berichterstattung: zB. Berichterstattung and das Finanzministerium, Vollständigkeit Berichterstattung, inhaltliche Richtigkeit der Berichterstattung, Überprüfung und Genehmigung, zeitlich korrekte Übermittlung Interne Berichterstattung: Vollständigkeit Berichterstattung, inhaltliche Richtigkeit der Berichterstattung, Überprüfung und Genehmigung Inhalte, zeitlich korrekte Übermittlung Vollständigkeit und Richtigkeit der Jahresabschlusserstellung
	Rechnungslegung: Perioden- / Jahresabschluss	Kontenanlage, Kontenabstimmung, manuelle Abschlussbuchungen und deren Überprüfung und Genehmigung, Genehmigungsmatrix, Vollständigkeit der Abschlussbuchungen, Abschlusscheckliste, Abweichungsanalyse Bilanz und GuV (Veränderungsanalyse) inkl. Erklärung von Abweichungen, Abgleich genehmigte Mittel mit Ausführung, Vollständigkeit der Belege/Rechnungen, Überprüfung Einhaltung der Vorgaben
	Rechnungslegung: Debitorenmanagement	Debitorenstammdaten: Anlage und Änderungen von Debitorenstammdaten, Mindesterfordernisse (zB. Schriftlichkeit der Änderungsgrundlage), Berechtigungen und 4-Augen-Prinzip bei kritischen Stammdatenänderungen, Validierung der Debitorenstammdaten (zB. Richtigkeit der Bankkontonummer), Stammdatenmanagement Rechnungsverarbeitung: Ausgangsrechnungsworkflow, Ausgangsrechnungsprüfung und Genehmigung von ergebniswirksamen Gutschriften, Genehmigungsmatrix, berechtigte Personen für die Genehmigung von Rechnungen und Gutschriften, Ausstellung von Rechnungen, Ausgangsrechnungsverbuchung, Periodenrichtiger Ausweis, Vollständigkeit Fakturierung Forderungsmanagement: Bonitätsbeurteilung, Blockieren von Debitoren, Mahnwesen, Mahnsperren, Überwachung überfällige Forderungen, Altersstrukturanalyse, Wertberichtigung und Abschreibung von Forderungen, Verarbeitung von Zahlungseingängen, Forderungsausgleich, Umgang mit zuordenbaren erhaltenen Zahlungen, kreditorische Debitoren, Saldenabstimmung
	Rechnungslegung: Kreditorenmanagement	Lieferantenstammdaten: Anlage und Änderungen von Lieferantenstammdaten, Mindesterfordernisse (zB. Schriftlichkeit der Änderungsgrundlage), Berechtigungen und 4-Augen-Prinzip bei kritischen Stammdatenänderungen, Validierung der Lieferantenstammdaten (zB. Richtigkeit der Bankkontonummer), Stammdatenmanagement Rechnungsverarbeitung: Eingangsrechnungsworkflow, Eingangsrechnungsprüfung (fachlich, formal, inhaltlich), Abgleich Rechnung/Bestellung/Lieferschein, Umgang mit Abweichungen, Eingangsrechnungsfreigabe (Freigabeworkflow), Genehmigungsmatrix, berechtigte Personen für die Genehmigung von Rechnungen, Eingangsrechnungsverbuchung, Periodenrichtiger Ausweis Durchführung von Zahlungen: Zahlungsplan/Zahlungsmanagement, Durchführung von Zahlungen, Freigabe von Zahlungen, Blockieren von Zahlungen, manuelle Zahlungen, Zahlungen mittels Zahlungsvorschlagsliste, Kontenabstimmung und Zuordnung von Zahlungen zu den offenen Posten, debitorische Kreditoren, Saldenabstimmung
	Veranlagung	Veranlagungsstrategie, Genehmigung von Veranlagungen, laufende Überwachung von Veranlagungen
	Liquiditätssicherung	Existenz und Qualität der Liquiditätsplanung, Genauigkeit des Liquiditäts-Forecastings, Bankkonten, Fristenkontrolle für Zahlungsverpflichtungen, Sicherstellung von Kreditlinien und Liquiditätsreserven, Einhaltung von Fördermittelauflagen, Trennung von Dritt- und Eigenmitteln, Regelmäßige Berichte an Leitungsorgan (Liquiditätsstatus, Risiken, Prognosen), Abweichungsanalysen
	Handkassenprüfung	Existenz und Qualität einer Kassenordnung, Führung eines Kassenbuchs, Vollständigkeit der Belege (formelle und materielle Prüfung, Verwendungszweck), Kassensturz (Vergleich Bargeldbestand und Kassenbuch), 4-Augen-Prinzip bei Kassenprüfung, Dokumentation der Prüfung
	Bankgarantieüberprüfung	Dokumentation aller Bankgarantien, Vollständigkeit und Aktualität der Dokumentation, Abgleich mit Verträgen (Garantiebeträge, Laufzeiten), Überwachung von Ablaufdaten (Verlängerung oder Rückgabe), Fristenmanagement und Benachrichtigungskonzept, Prüfung der Garantiebeträge und Bankbonität, 4-Augen-Prinzip bei Annahme und Rückgabe von Garantien, Klare Kompetenzregelungen, regelmäßige Berichte an Leitungsorgan
Drittmittel und Fundraising	Drittmittelprojekte	Drittmittelbeschaffung, Akquise von Drittmittelzuschüsse (Angebot, Überprüfung und Annahme), Drittmittelverwaltung, Dritmittelverwendung, Beendigung
IT-Nutzung	Manage Access / Benutzerverwaltung	Manage Access bezieht sich auf die Kontrollen und Prozesse, die den Zugriff auf IT-Systeme und -Daten regeln, um sicherzustellen, dass nur autorisierte Benutzer Zugang haben, Benutzerzugriffsverwaltung, Authentifizierungs- und Autorisierungsprozesse, regelmäßige Überprüfung von Zugriffsrechten, Passwortsettings, Rechtevergabe, Rechteänderung, Rechteentzug / Löschung von Benutzer, Regelmäßiges Review von Rechten Beinhaltet auch die Userberechtigungen der IT-Mitarbeiter, Hard- und Software wie zB USB-Sticks, externe Speichermedien, 2-Faktor Authentifizierung, Passwortstrategie etc. SAP-Funktionentrennung: dokumentiertes Rollen- und Berechtigungskonzept, Rechte-Rollen-Review, Notfallberechtigungen, Identifikation und Trennung kritischer Funktionen, Prüfung auf Doppelrollen, dokumentierte Ausnahmen, Einsatz von SAP-Tools zur SoD-Prüfung
	Manage Change	Manage Change bezieht sich auf die Prozesse und Kontrollen, die sicherstellen, dass alle Änderungen an IT-Systemen und -Anwendungen ordnungsgemäß verwaltet, dokumentiert, getestet und genehmigt werden, Änderungsanforderungen, Genehmigungsprozesse, Testprotokolle und Dokumentation
	Manage Operations	Manage Operations umfasst die Überwachung und Verwaltung der täglichen IT-Betriebsaktivitäten, um sicherzustellen, dass IT-Systeme zuverlässig und effizient funktionieren, Systemüberwachung, Backup- und Wiederherstellungsverfahren, Vorfallmanagement und Leistungsüberwachung
Personaladministration und Reisen	Mitarbeitereintritt	Einstellungsprozess, Richtlinien zum Einstellungsprozess, Eintrittscheckliste, Vertragsmanagement, IT- und Systemzugänge, Onboarding und Schulungen
	Stammdatenpflege	Anlage und Änderungen von Mitarbeiterstammdaten, Mindesterfordernisse (zB. Schriftlichkeit der Änderungsgrundlage), Berechtigungen und 4-Augen-Prinzip bei kritischen Stammdatenänderungen
	Zeiterfassung / Überstunden	Zeiterfassung, Überprüfung und Genehmigung der Zeiterfassung, Umgang mit Überstunden, Genehmigung von Überstunden
	Gehaltsabwicklung/ -verrechnung	Durchführung der laufenden Gehaltsabrechnung, variable Gehaltsbestandteile, Genehmigung und Kontrolle von Gehaltsauszahlungen, Schnittstellen zu externen Dienstleistern
	Reiseabwicklung / Reisekostenabrechnung	Reisekostenrichtlinie, Genehmigung von Dienstreisen, Abrechnung von Dienstreisen, erforderliche Dokumente zur Abrechnung
	Personalrückstellungen	Berechnung und Verbuchung von Personalrückstellungen, Überprüfung und Freigabe der Berechnung und Verbuchung von Personalrückstellungen, Korrektheit von Basisdaten, Schnittstelle zu externen Dienstleistern
	Mitarbeiteraustritt	Austrittsprozess, Austrittscheckliste, Umgang mit Hard- und Software sowie Zutritts- und Systemberechtigungen