MITTEILUNGSBLATT

der
UNIVERSITÄT GRAZ

50. SONDERNUMMER

Studienjahr 2023/24 | Ausgegeben am 20. 03. 2024 | 23.b Stück

Richtlinie

für das interne Kontrollsystem

Betrieb des an der Universität Graz eingesetzten SAP-Systems

Beschluss des Rektorats vom 14.03.2024

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.

Richtlinie für das interne Kontrollsystem

Betrieb des an der Universität Graz eingesetzten SAP-Systems

Version 1.0	**Erstellung der Richtlinie**	Mag. Andreas Doppler
		Mag. Sandra Hungerländer
		Mag. Manfred Ortner
	Prüfung der Richtlinie	Mag. Christa Peissl
	Genehmigung der Richtlinie	Mag. Ralph Zettl

Version 2.0	**Überarbeitung der Richtlinie**	Mag. Andreas Doppler
		Mag. Sandra Hungerländer-Kropf
		Mag. Manfred Ortner
	Durchsicht und Anregungen	Interne Revision
	Genehmigung der Richtlinie	Mag. Ralph Zettl

Version 3.0	**Überarbeitung der Richtlinie**	Mag. Andreas Doppler
		Mag. Sandra Hungerländer-Kropf
		Mag. Manfred Ortner
	Durchsicht und Anregungen	Interne Revision
	Genehmigung der Richtlinie	Mag. Ralph Zettl

Version 4.0	**Überarbeitung der Richtlinie**	**Mag. Andreas Doppler**
		Mag. Sandra Hungerländer-Kropf
		Mag. Manfred Ortner
	Durchsicht und Anregungen	**Interne Revision**
	Genehmigung der Richtlinie	**Mag. Ralph Zettl**

Version 5.0	**Überarbeitung der Richtlinie**	Mag. Andreas Doppler
		Mag. Sandra Hungerländer-Kropf
		Mag. Manfred Ortner
	Durchsicht und Anregungen	Interne Revision
	Genehmigung der Richtlinie	Mag. Ralph Zettl

Version 5.0, 20.03.2024

Änderungsverzeichnis

Version	Datum	Änderung	erstellt von
0.1	15.09.2005	Erstellung der IKS-Richtlinie	Mag. Andreas Doppler, Mag. Sandra Hungerländer, Mag. Manfred Ortner
0.2	13.10.2005	Endredaktion der IKS-Richtlinie	Mag. Andreas Doppler, Mag. Sandra Hungerländer, Mag. Manfred Ortner
1.0	24.10.2005	Erstellung der Endfassung der IKS-Richtlinie zur Veröffentlichung	Mag. Andreas Doppler, Mag. Sandra Hungerländer, Mag. Manfred Ortner
2.0	05.05.2011	Einarbeitung der Prüfungsergebnisse der SAP-Revision	Mag. Andreas Doppler, Mag. Sandra Hungerländer-Kropf, Mag. Manfred Ortner
3.0	29.08.2014	Aktualisierung auf Grund der Umstellung auf den direkten SAP Einstieg und Einführung von ESS – Employee Selfservice	Mag. Andreas Doppler, Mag. Sandra Hungerländer-Kropf, Mag. Manfred Ortner
4.0	19.09.2018	Aktualisierung auf Grund der SSO-Anmeldung für ESS-Benutzer:innen	Mag. Andreas Doppler, Mag. Sandra Hungerländer-Kropf, Mag. Manfred Ortner
5.0	20.03.2024	Aktualisierung auf Grund der Änderung der Lizenzbedingungen	Mag. Andreas Doppler, Mag. Sandra Hungerländer-Kropf, Mag. Manfred Ortner

Abkürzungsverzeichnis

Abkürzung	Bedeutung
ACOnet	Austrian Academic Computer Network
BRZ	Bundesrechenzentrum
BuBi	Abteilung für Buchhaltung und Bilanzierung
BW	Business Warehouse
CCC	Customer Competence Center
CO	Controlling
CoRe	Abteilung für Controlling und Ressourcenplanung
ERP-System	Enterprise Resource Planning System
ESS	Employee Selfservice
FI	Finanzwesen (Finance)
FI-AA	Finanzwesen-Anlagenbuchhaltung (Finance Asset Accounting)
HR	Personalwesen (Human Resources)
ICR	Interner Change Request
IKS	Internes Kontrollsystem
LDAP	Lightweight Directory Access Protocol
MM	Materialmanagement
MSS	Management Selfservice
PeCo	Abteilung für Personalcontrolling
PIN	Persönliche Identifikationsnummer
PU1	Produktivsystem
QU1	Qualitätssicherungssystem
SAML	Security Assertion Markup Language
SAP	Systems, Applications, Products in Data Processing
SD	Verkauf (Sales and Distribution)
SLA	Service Level Agreement
SLF-System	Support Line Feedback System
SSL	Secure Sockets Layer
SSO	Single Sign On
TU1	Entwicklungssystem
uniIT	uniIT (Informationsmanagement)
VM	Vertragsmanagement (Contract Management)
VPN	Virtual Private Network

Definitionen

Applikationsverantwortliche/r	Trägt die Verantwortung für die Entwicklungsarbeiten sowie die Konzeption und Realisierung des Weiterausbaus von SAP
Benutzer:innen- und Berechtigungsverwaltung	Ist für die gesamte Administration der SAP-Zugänge sowie für die Anwender:innenbetreuung zuständig
Berichtsuser:in	SAP-Benutzer:innen, die definierte SAP-Berichte aufrufen
Betriebskoordinator:innen	Sind für die Organisation und Sicherstellung des SAP-Betriebs verantwortlich
CCC-Mitarbeiter:innen	Mitarbeiter:innen des BRZ, die die SLF-Meldungen der Universität annehmen und bearbeiten
CO-Kontierung	Kostenstellen und Innenaufträge
Customizing	Anpassung der Standardsoftware auf die Geschäftsprozesse des Kunden/der Kundin
Data Dictionary	Ermöglicht eine zentrale Beschreibung und Verwaltung aller im System verwendeten Daten
Dateneigentümer:innen	Personen, die für bestimmte CO-Kontierungen gem. Unterschriftenprobeblatt anweisungsberechtigt sind
Debug-Modus	Ermöglicht eine Ablaufverfolgung des zu untersuchenden Programmes in einzelnen Schritten oder zwischen definierten Haltepunkten
e-Banking	Zahlungsverkehr und Bankgeschäfte werden beleglos in elektronischer Form abgewickelt
ESS-Benutzer:innen	Personen, die benutzerspezifische Szenarien in ESS - Employee Selfservice, benutzerspezifische Szenarien in MSS – Manager Selfservice und/oder die Genehmigungsworkflows in SAP nutzen.
First Level Support	Erste Auskunftsstelle für die/den SAP-Benutzer:in bei Problemen
ITS (Internet Transaction Server)	Wandelt die Daten in eine Form um, die in Webbrowsern angezeigt werden können
MM/SD Light User:in	SAP-Benutzer:innen, die definierte Transaktionen in den Modulen MM und SD und/oder im Vertragsmanagement ausführen
PIN	Kennwort, das bei der Neuanlage eines/einer SAP-Benutzer:in bzw. beim Zurücksetzen eines gesperrten Kennwortes vergeben wird und das bei der erstmaligen Anmeldung im System geändert werden muss
Professional User:in	SAP-Benutzer:innen die modulübergreifend umfangreiche Transaktionen ausführen
SAP Account	SAP-Zugang

SAP-Benutzer:innen	Personen, welche im SAP-System operative Transaktionen ausführen. SAP-Benutzer:innen sind: Professional User:in MM/SD-Light User:in Berichtsuser:in
SAP GUI	Benutzeroberfläche (Graphical User Interface), welche die Schnittstelle zwischen SAP-Benutzer:innen und dem SAP-System bildet
SAP Server	Hardware, auf der das SAP-System installiert ist
Secure Sockets Layer SSL	Secure Sockets Layer (SSL) ist ein Verschlüsselungsprotokoll für Datenübertragungen im Internet
Security Policy der uniIT	Regelwerk der uniIT, mit dem die IT-Sicherheit an der Universität gewährleistet werden soll
SLA-Report	Vom BRZ monatlich erstellter Report, in dem die Kriterien des Service Level Agreements und die durchgeführten Transporte aufgelistet sind
SLF-System	Ein Tool, mit dem alle Supportmeldungen der Key User:innen des BRZs abgewickelt und dokumentiert werden
Support Mitarbeiter:innen des BRZ	Siehe CCC-Mitarbeiter:innen
VPN	VPN steht für "Virtual Private Network" oder "virtuelles privates Netzwerk" und bietet eine sichere und verschlüsselte Verbindung über ein öffentliches Netz

Inhaltsverzeichnis

1 Ziele und Zielgruppe, Zeitpunkt des In-Kraft-Tretens

Die vorliegende Richtlinie für das Interne Kontrollsystem (IKS) enthält die Regelungen, die einen

- sicheren,
- ordnungsmäßigen und
- wirtschaftlichen

Betrieb des an der Universität Graz eingesetzten SAP-Systems gewährleisten.

Die Richtlinie gilt für alle Personen, für deren Tätigkeit ein Zugriff auf das SAP- und/oder ESS-System erforderlich ist.

Die Richtlinie trat am 7. November 2005 in Kraft und galt bis zur Veröffentlichung der Version 2.0.

Die Version 2.0 trat am 25.05.2011 mit der Veröffentlichung im Mitteilungsblatt in Kraft und galt bis zur Veröffentlichung der Version 3.0.

Die Version 3.0 trat am 24.09.2014 mit der Veröffentlichung im Mitteilungsblatt in Kraft und galt bis zur Veröffentlichung der Version 4.0.

Die Version 4.0 trat am 19.09.2018 mit der Veröffentlichung im Mitteilungsblatt in Kraft und galt bis zur Veröffentlichung der Version 5.0.

Die Version 5.0 tritt mit Veröffentlichung im Mitteilungsblatt in Kraft und gilt bis auf Widerruf.

2 Produktivsystem (PU1)

2.1 IKS-Bereich: Sicherheit

Im IKS-Bereich Sicherheit können insbesondere folgende Risiken auftreten:

- **Zugriff auf SAP-Daten durch unberechtigte Personen**
  Der unberechtigte Zugriff auf SAP-Daten kann sowohl durch Mitarbeiter:innen der Universität als auch durch externe Personen erfolgen. Ursachen für den unberechtigten Zugriff auf SAP-Daten sind zu weit gefasste Berechtigungen eines/r SAP-Benutzer:in oder Angriffe auf das Netzwerk und einzelne PCs. Mögliche Gefahrenquellen befinden sich daher innerhalb und außerhalb der Universität.

- **Datenschutzverletzungen**
  Da im SAP-System personenbezogene Daten verarbeitet werden, besteht die Gefahr von Datenschutzverletzungen.

Die im IKS-Bereich Sicherheit definierten Regelungen zur

- Netzwerksicherheit,
- Anmeldesicherheit und
- Berechtigungsverwaltung

sollen diesen Risiken entgegenwirken.

2.1.1 Netzwerksicherheit

Die Regelungen zur Netzwerksicherheit legen die Abläufe hinsichtlich

- Kommunikation zwischen Arbeitsplatzrechner und SAP-Server sowie die
- Einhaltung der Security Policy für Computer und Netze

fest.

2.1.1.1 Kommunikation zwischen Arbeitsplatzrechner und SAP-Server

Die Kommunikation zwischen den Arbeitsplatzrechnern an der Universität Graz und den SAP-Servern im BRZ erfolgt über das ACOnet. Die Verbindung zwischen Arbeitsplatzrechner und VPN-Appliances und im ACOnet muss verschlüsselt erfolgen. Die Verschlüsselung im ACOnet wird hierzu über eine Lan-To-Lan-Verbindung hergestellt. Dazu stellt das BRZ zwei Lan-To-Lan-Router für die Kommunikation zwischen der Universität Graz und dem BRZ zur Verfügung. Die Verschlüsselung von den SAP-Clients in die Rechenzentren der Universität erfolgt über Cisco SSL VPN Clients zu redundanten VPN Appliances der Universität. Für die Cisco SSL VPN Clientanmeldung ist eine Multifaktor Authentifizierung eingerichtet.
Zusätzlich ist eine Verschlüsselung zwischen Arbeitsplatzrechner und SAP-Servern im BRZ auch durch die Secure Network Communication im SAP GUI gewährleistet.

Die Herstellung einer gesicherten Verbindung über Lan-To-Lan bis inkl. der Lan-To-Lan Router an der Universität ist Aufgabe des Bundesrechenzentrums.[1] Für den Teil nach den Lan-To-Lan Routern bis zu den Clients ist die uniIT zuständig. Aufgabe des SAP-Betriebskoordinatorenteams an der Universität ist es, einmal wöchentlich das Vorhandensein der gesicherten Verbindung zu überprüfen. Die Überprüfung erfolgt, indem versucht wird, sich ohne gesicherte Verbindung am System anzumelden.

Der sichere Zugang zum SAP GUI for HTML, NetWeaver Business Client und Fiori Launchpad erfolgt über Secure Sockets Layer (SSL).

2.1.1.2 Einhaltung der Security Policy der uniIT

Um den Zugriff auf SAP-Daten durch unberechtigte Personen zu verhindern, ist die Security Policy der uniIT einzuhalten. Die Security Policy der uniIT ist unter https://online.uni-graz.at/kfu_online/wbMitteilungsblaetter.display?pNr=75196 einsehbar. Für den Inhalt und die Umsetzung der Security Policy sind die dafür zuständigen Mitarbeiter:innen der uniIT verantwortlich.

2.1.2 Anmeldesicherheit[2]

Die Regelungen zur Anmeldesicherheit legen die Abläufe hinsichtlich

- Anlage der SAP-Benutzer:innenstammdaten,
- Anlage der ESS-Benutzer:innenstammdaten,
- Kennwortregelung für SAP-Benutzer:innen,
- Kennwortregelung für ESS-Benutzer:innen,
- Sperren, Freischalten und Löschen von SAP-Zugängen,
- Sperren, Freischalten und Löschen von ESS-Zugängen,
- SAP-Zugänge für Mitarbeiter:innen des BRZ,
- SAP-Zugänge für Mitarbeiter:innen von Beratungsfirmen und sonstigen externen Stellen

fest.

Im Bereich Anmeldesicherheit wird zwischen SAP- und ESS-Benutzer:innen unterschieden, da sich die Prozesse zum Anlegen, Sperren und Löschen bei diesen beiden Benutzer:innengruppen unterscheiden.
SAP-Benutzer:innen sind jene Benutzer:innen, welche im SAP-System operative Transaktionen ausführen.
ESS-Benutzer:innen hingegen nutzen in SAP die Employee Selfservices, Manager Selfservices und die Genehmigungsworkflows. Das heißt, diese Benutzer:innen sind mit keinen individuellen Berechtigungsrollen ausgestattet.

[1] vgl. Anhang, Kapitel 5.3: Auszug aus Angebot „VPN-Anbindung“
[2] vgl. Anhang Kapitel 5.2.2.1: Prozess IKS1 – Neuer SAP-Zugang
vgl. Anhang Kapitel 5.2.2.2: Prozess IKS2 – Neuer ESS-Zugang
vgl. Anhang Kapitel 5.2.2.3: Prozess IKS3 – Passwort zurücksetzen
vgl. Anhang Kapitel 5.2.2.4: Prozess IKS4 – Sperren, Freischalten und Löschen eines SAP-Zugangs

2.1.2.1 Anlage der SAP-Benutzer:innenstammdaten

Die Vergabe von SAP-Accounts erfolgt ausschließlich auf Basis des Antragsprozesses.
Für Berichts- und MM/SD Light User:innen ist der Antrag durch eine/einen Dateneigentümer:in zu genehmigen, auf deren/dessen Daten durch die einzurichtenden Berechtigungen der Zugriff ermöglicht wird. Dateneigentümer:innen sind Anweisungsberechtigte lt. Unterschriftenprobenblatt.
Der Antrag für Professional User:innen ist durch den/die Vorgesetzte/n des/der Antragsteller:in sowie durch die Dateneigentümer:innen zu genehmigen.

Die Genehmigung des/der Dateneigentümer:in ist notwendig, um den Datenschutz zu gewährleisten.

Von der Genehmigungspflicht durch die Dateneigentümer:innen ausgenommen sind Professional User:innen der BuBi, der CoRe, der PeCo, der Wirtschaftsabteilung, des Personalressorts, der Abteilung für Gebäude und Technik, der Internen Revision, des Forschungsmanagement und -service sowie des Competence Center SAP, da diese Personen ändernden oder anzeigenden Zugriff auf alle Kostenstellen und Innenaufträge der Universität im Rahmen der ihnen zugeordneten Rollen benötigen.

Der/die Antragsteller:in muss ein bestehendes Dienstverhältnis zur Universität Graz haben.

Alle Anträge auf einen SAP-Zugang sind von der Benutzer:innen- und Berechtigungsverwaltung hinsichtlich Vollständigkeit und Freigaben zu prüfen. Anträge von Professional User:innen sind zusätzlich vom Betriebskoordinatorenteam in Hinblick auf die Vereinbarkeit mit den, in dieser Richtlinie genannten Regelungen und das Auftreten von kritischen Berechtigungen zu prüfen. Erst nach Freigabe des Antrags durch den/die Applikationsverantwortliche/n darf der SAP-Zugang im System angelegt werden.

Bevor der/dem neu angelegten SAP-Benutzer:in die Zugangsdaten übermittelt werden, ist im Sinne des 4-Augen-Prinzips von einer/einem weiteren Mitarbeiter:in der Benutzer:innen- und Berechtigungsverwaltung zu prüfen, ob die beantragten Berechtigungen im SAP-System richtig vergeben wurden und die Richtigkeit ist zu bestätigen.

2.1.2.2 Anlage der ESS-Benutzer:innenstammdaten

Ab dem Zeitpunkt, an welchem

- ein neuer Personalstammsatz im HR angelegt wurde
- die Emailadresse im IT 0105 (Subtyp 0010) gepflegt wurde
- das Beginndatum des Dienstverhältnisses <= Tagesdatum ist
- das Endedatum des Dienstverhältnisses > Tagesdatum ist
- das Dienstverhältnis nicht in einer Z-Tabelle (Mitarbeitergruppe, Mitarbeiterkreis, Anstellungsverhältnis) als Ausnahme definiert ist und
- der Abrechnungskreis ungleich 99 ist

wird ein ESS-Zugang für die/den Mitarbeiter:in angelegt.

2.1.2.3 Kennwortregelung für SAP-Benutzer:innen

Wenn ein(e) ESS-Benutzer:in in SAP operative Tätigkeiten ausführen soll, wird der ESS-Zugang in einen SAP-Zugang umgewandelt.
Für jede/n neue/n SAP-Benutzer:in muss ein eigener PIN generiert werden. Ansonsten besteht die Gefahr, dass mit einem allgemein bekannten PIN Anmeldungen unter dem neu angelegten Benutzernamen von nicht berechtigten Personen vorgenommen werden.

Verfahren zur Vergabe des PINs
Der PIN ist immer achtstellig und besteht aus einer Buchstaben-Zahlenkombination. Wird ein/e neue/r SAP-Benutzer:in angelegt, wird von der Benutzer:innen- und Berechtigungsverwaltung der PIN generiert. Dieser wird in einer SAP-Datenbanktabelle mit dem SAP-Benutzernamen verschlüsselt gespeichert. Die Speicherung des PIN ist notwendig, weil beim Freischalten eines gesperrten Kennwortes per Telefon/E-Mail der PIN die eindeutige Identifikation der SAP-Benutzerin/des SAP-Benutzers sicherstellt.
Die SAP-Benutzer:innen erhalten den PIN per E-Mail mitgeteilt. Der PIN muss von den SAP-Benutzer:innen bei der erstmaligen Anmeldung geändert werden.

Benutzer:innenkennwort
Das von der/dem Benutzer:in verwendete Kennwort muss aus mind. 8 Zeichen bestehen, wobei mind. 2 Buchstaben und mind. 2 Ziffern vorkommen müssen. Vom System wird nach 120 Tagen eine Kennwortänderung verlangt.

2.1.2.4 Kennwortregelung für ESS-Benutzer:innen

ESS-Benutzer:innen melden sich im System über Single Sign On mittels SAML mit den LDAP-Zugangsdaten dh mit ihrem Uni-Graz-Account an. Somit gelten für ESS-Benutzer:innen die Kennwortregelungen (Mindestanforderungen, Kennwortänderung, Multifaktor Authentifizierung, usw.) welche für die SSO-Systeme der uniIT gelten.

2.1.2.5 Sperren, Freischalten und Löschen von Zugängen der SAP-Benutzer:innen

Falscheingabe des Kennworts
Der SAP-Zugang wird durch das System automatisch gesperrt, wenn bei der Anmeldung von der/dem SAP-Benutzer:in das Passwort dreimal falsch eingegeben wurde.

In diesem Fall ist von der/dem gesperrten SAP-Benutzer:in Kontakt mit der Benutzer:innen- und Berechtigungsverwaltung aufzunehmen, die das Passwort entsperrt, wenn der/die SAP-Benutzer:in die ersten vier Zeichen des ursprünglich vergebenen PINs bekannt gibt (schriftlich oder telefonisch).

Sind auch die ersten vier Zeichen des PINs nicht mehr bekannt, kann das Kennwort nur nach einem schriftlichen Antrag des/der SAP-Benutzer:in an die Benutzer:innen- und Berechtigungsverwaltung entsperrt werden.

Kennwort ist der/dem SAP-Benutzer:in nicht mehr bekannt
Von der/dem SAP-Benutzer:in ist Kontakt mit der Benutzer:innen- und Berechtigungsverwaltung aufzunehmen, die das Passwort zurücksetzt, wenn der/die SAP-Benutzer:in sich an das Kennwort nicht mehr erinnern kann. Dabei sind die ersten vier Zeichen des ursprünglich vergebenen PINs bekannt zu geben (schriftlich oder telefonisch). Sind auch die ersten vier Zeichen des PINs nicht mehr bekannt, kann das Kennwort nur nach einem schriftlichen Antrag des/der SAP-Benutzer:in an die Benutzer:innen- und Berechtigungsverwaltung entsperrt werden.

Beendigung des Dienstverhältnisses, organisatorische Änderungen
Bei der Beendigung des Dienstverhältnisses darf auch der SAP-Zugang des/der jeweiligen Mitarbeiter:in nicht mehr möglich sein. Ändert sich der Aufgabenbereich des/der SAP-Benutzer:in derart, dass kein SAP-Zugang mehr benötigt wird, ist der SAP-Zugang zu löschen. Daher ist in diesen Fällen die Benutzer:innen- und Berechtigungsverwaltung von der/dem jeweiligen Vorgesetzten mittels Formular zu verständigen.

Von der Benutzer:innen- und Berechtigungsverwaltung muss monatlich geprüft werden, ob ein SAP-Zugang an eine Person vergeben ist, deren Beschäftigungsverhältnis geendet hat oder deren organisatorische Zuordnung sich geändert hat.
Bei der Änderung der organisatorischen Zuordnung ist mit dem/der bisherigen Vorgesetzten abzuklären, was mit dem SAP-Zugang geschehen soll, falls noch kein Formular bei der Benutzer:innen- und Berechtigungsverwaltung eingelangt ist.

Für die beiden oben angeführten Prüfungen werden jeweils eigenentwickelte SAP-Reports eingesetzt.

Keine Anmeldung in SAP über einen längeren Zeitraum hinweg
Von der Benutzer:innen- und Berechtigungsverwaltung ist monatlich zu prüfen, ob SAP-Benutzer:innen seit 60 Tagen nicht mehr angemeldet waren. Diese SAP-Benutzer:innen sind darauf hin zu sperren. Es ist dann zu klären, ob diese SAP-Benutzer:innen im System gelöscht werden sollen. SAP-Benutzer:innen, deren letzte Anmeldung 6 Monate zurückliegt, sind zu löschen.

2.1.2.6 Sperren, Freischalten und Löschen von Zugängen der ESS-Benutzer:innen

Da die ESS-Benutzer:innen das LDAP-Kennwort zur Anmeldung in ESS verwenden, gelten für das Sperren und Freischalten der LDAP-Kennwörter die entsprechenden Regelungen der uniIT[3].

Wenn ein Dienstverhältnis endet, ist eine Anmeldung über Single Sign On nicht mehr möglich. Ein Dienstverhältnis gilt als beendet, wenn das Endedatum des Dienstverhältnisses < Tagesdatum ist.

Die Zugänge werden regelmäßig nach Ablauf eines definierten Zeitfensters gelöscht.

[3] siehe https://intranet.uni-graz.at/einheiten/715/services/Pages/SEC_benutzungsordnung.aspx

2.1.2.7 SAP-Zugänge für Mitarbeiter:innen des BRZ

Die SAP-Zugänge von Support-Mitarbeiter:innen des BRZ werden vom BRZ verwaltet. Die Richtlinien für die Vergabe und den Umfang der Berechtigungen von Support-Mitarbeiter:innen müssen in einem Sicherheitskonzept des BRZ enthalten sein.[4]

Die Benutzer:innen- und Berechtigungsverwaltung der Universität muss vom BRZ benachrichtigt werden, wenn wesentliche Veränderungen an den Berechtigungen von Support-Mitarbeiter:innen des BRZ vorgenommen werden.
Die Betriebskoodinator:innen prüfen monatlich die Einhaltung der in der Richtlinie festgelegten Namenskonventionen für die Mitarbeiter:innen des BRZ und deren Rollenzuordnung.

Von den Betriebskoordinator:innen wird monatlich geprüft, ob von Mitarbeiter:innen des BRZ im Produktivsystem schreibende Zugriffe auf Applikationsdaten vorgenommen wurden.

2.1.2.8 SAP-Zugänge für Mitarbeiter:innen von Beratungsfirmen und sonstigen externen Stellen

Die SAP-Zugänge für Mitarbeiter:innen von Beratungsfirmen und sonstigen externen Stellen werden von der Benutzer:innen- und Berechtigungsverwaltung der Universität verwaltet. Diese Zugänge werden nach folgender Namenskonvention im System angelegt: B_EXT_*NACHNAME*. Der Benutzername ist maximal 12 Zeichen lang.

2.1.3 Berechtigungsverwaltung

Berechtigungen werden an der Universität über Rollen vergeben.

2.1.3.1 Berechtigungsverwaltung für SAP-Benutzer:innen

Die Rollen müssen funktional/organisatorisch so gestaltet sein, dass der/die Inhaber:in dieser Rolle alle in seinem Aufgaben- und/oder Verantwortungsbereich liegenden Tätigkeiten durchführen kann. Es ist bei der Definition der Rollen aber auch sicherzustellen, dass von der/dem Rolleninhaber:in jene Funktionen des Systems, die nicht für seine/ihre Arbeit benötigt werden, nicht ausgeführt werden können. Daher muss durch das Rollenkonzept verhindert werden, dass von Rolleninhaber:innen auf Daten zugegriffen werden kann, für die sie nicht berechtigt sind.

Die Regelungen zur Berechtigungsverwaltung legen die Abläufe hinsichtlich

- Detaillierungsgrad der Berechtigungen,
- Kritische Berechtigungen,
- Berechtigungsänderungen und
- Rollenänderungen

fest.

[4] vgl. BRZ UNISAP-Sicherheitskonzept V7.71, Seite 22 und UNISAP-Berechtigungskonzept V2.2 (Diese liegen bei den SAP-Betriebskoordinator:innen auf. Das Sicherheitskonzept und UNISAP-Berechtigungskonzept wird aufgrund von Vertraulichkeitserfordernissen dieser Richtlinie nicht beigelegt.)

2.1.3.1.1 Detaillierungsgrad der Berechtigungen

Das Berechtigungskonzept ist in SAP technisch so umzusetzen, dass Berechtigungen hierarchisch bis auf einzelne Transaktionen sowie Berechtigungsobjekte vergeben werden können.

2.1.3.1.2 Kritische Berechtigungen

Vom Betriebskoordinatorenteam sind Transaktionen und die entsprechenden Berechtigungsobjekte zu berücksichtigen, die nicht zusammen an eine Person vergeben werden dürfen, da sie zu kritischen Kombinationen von Berechtigungen führen würden.

Bei der Definition von kritischen Kombinationen von Berechtigungen sind auch Berechtigungen des/der SAP-Benutzer:in zu berücksichtigen, die diese/r in Non-SAP-Systemen hat (zB e-Banking).

2.1.3.1.3 Berechtigungsänderungen[5]

Bei der Änderung von Berechtigungen sind zwei Fälle zu unterscheiden:

- Änderung der Zugriffsberechtigung auf Kostenstellen und Innenaufträge und
- Änderungen der Rollenzuordnung von Professional User:innen.

Änderung der Zugriffsberechtigung auf Kostenstellen und Innenaufträge

Änderungen der Berechtigungen eines/r SAP-Benutzer:in zur Bearbeitung oder Anzeige von Kostenstellen oder Innenaufträgen dürfen nur vorgenommen werden, wenn ein Antrag entsprechend des Berechtigungsänderungsprozesses vorliegt, der von allen betroffenen Dateneigentümer:innen genehmigt ist. Ergeben sich Berechtigungsänderungen durch einen organisatorischen Wechsel der/des SAP-Benutzer:in, so ist im Antragsformular anzugeben, ob die bisherigen Berechtigungen belassen werden können.[6]

Von der Benutzer:innen- und Berechtigungsverwaltung ist monatlich zu überprüfen, ob für alle organisatorischen Änderungen, die SAP-Benutzer:innen betreffen, die entsprechende Änderung der Zugriffsberechtigung beantragt wurde. Dies geschieht mittels eines eigenentwickelten SAP-Reports.

Änderungen der Rollenzuordnung von Professional User:innen

Bei der Zuordnung der Rollen ist darauf zu achten, dass es zu keiner Funktionshäufung kommt, die zu kritischen Berechtigungen des/der einzelnen SAP-Benutzer:innen führt. Alle Anträge auf Berechtigungsänderungen, die Professional User:in betreffen, sind daher vom Betriebskoordinatorenteam zu prüfen und von der/dem Applikationsverantwortlichen zu genehmigen.

Bevor die/der SAP-Benutzer:in über die Berechtigungsänderung informiert wird, ist im Sinne des 4-Augen-Prinzips von einer/einem weiteren Mitarbeiter:in der Benutzer:innen- und Berechtigungsverwaltung zu prüfen, ob die beantragte Berechtigungsänderung im SAP-System richtig umgesetzt wurde und die Richtigkeit ist zu bestätigen.

[5] vgl. Anhang Kapitel 5.2.2.6: Prozess IKS6 – Berechtigungsänderung
[6] vgl. Anhang Kapitel 5.2.2.5: Prozess IKS5 – Übertragung eines SAP-Zugangs

2.1.3.1.4 Rollenänderungen[7]

Das Betriebskoordinatorenteam muss vor der technischen Umsetzung der Rollenänderung die Änderung des Funktionsumfangs einer Rolle prüfen. Es muss geprüft werden, ob kritische Kombinationen von Berechtigungen innerhalb der Rolle oder in Kombination mit anderen Rollen auftreten können.

Nach der Prüfung der Rollenänderung durch das Betriebskoordinatorenteam muss der/die Applikationsverantwortliche die Änderung schriftlich genehmigen.

Bevor die geänderte Rolle in das Produktivsystem transportiert wird, ist im Sinne des 4-Augen-Prinzips von einer/einem weiteren Mitarbeiter:in der Benutzer:innen- und Berechtigungsverwaltung zu prüfen, ob die beantragte Rollenänderung im SAP-System richtig umgesetzt wurde, und die Richtigkeit ist zu bestätigen.

2.1.3.1.5 Periodische Autorisierung der Rollenvergabe

Um sicherstellen zu können, dass die Rollenvergabe noch den tatsächlichen Aufgabenbereichen der Professional User:innen entspricht, wird den LeiterInnen jener Einheiten, in denen Mitarbeiter:innen über einen Professional User verfügen, in periodischen Abständen (halbjährlich) die Information, welche Mitarbeiter:in welche Rollen zugeordnet hat und welche Transaktionen in den einzelnen Rollen enthalten sind, zur Verfügung gestellt.

Diese Zuordnungen sind von den LeiterInnen zu bestätigen und der Benutzer:innen- und Berechtigungsverwaltung zu übermitteln.

2.1.3.2 Berechtigungsverwaltung für ESS-Benutzer:innen

ESS-Benutzer:innen erhalten einheitliche, nicht benutzerspezifisch ausgeprägte Rollen je nach Art des Dienstverhältnisses. In den Rollen sind das Menü und die Berechtigungen für die einzelnen Applikationen für ESS - Employee Selfservice, MSS – Manager Selfservice und für Genehmigungsprozesse abgebildet.

Die Einschränkung der Berechtigungen in den einzelnen Applikationen von ESS und MSS erfolgt über die Zuordnung der jeweiligen Person im Organisationsmanagement im Modul HR. Das heißt, über diese Zuordnungen ist gewährleistet, dass die ESS-Benutzer:innen nur die für sie vorgesehenen Aktivitäten ausführen bzw. Daten einsehen können.

Für die Genehmigungsprozesse sind keine benutzerspezifischen Berechtigungs-einschränkungen in den Rollen notwendig, da die Benutzer:innenfindung auf Grund des im jeweiligen Workflow festgelegten Regelwerkes erfolgt[8].

[7] vgl. Anhang Kapitel 5.2.2.7: Prozess IKS7 – Rollenänderung

[8] siehe „Rahmenbetriebsvereinbarung über den Einsatz der Informations- und Kommunikationstechnologie im Arbeitsprozess an der Universität Graz (RBV IKT): Anhang SAP“

2.2 IKS-Bereich: Ordnungsmäßigkeit

Im IKS-Bereich Ordnungsmäßigkeit können insbesondere folgende Risiken auftreten:

- **Die Nachvollziehbarkeit von Aktivitäten im SAP-System ist nicht gegeben.** Eine Ursache für die mangelnde Nachvollziehbarkeit kann das Fehlen einer Dokumentation von Eigenentwicklungen oder die fehlende Weitergabe von Informationen über vorgenommene Systemeinstellungen durch das BRZ sein.

- **Fehlerhaft arbeitende Schnittstellen**
  Daten aus Vorsystemen werden unvollständig, redundant oder nicht zeitnah in SAP übernommen

- **Fehler im Ablauf der Anwendungsentwicklung**
  Eigenentwicklungen werden ohne Freigabeverfahren ins Produktivsystem transportiert oder die Anwendungsentwicklung erfolgt direkt im Produktivsystem. Es besteht weiters das Risiko, dass das Freigabeverfahren durch Änderung der Entwicklung auf QU1 beeinflusst wird. Wenn diese Änderungen nicht auf TU1 1:1 nachgezogen werden, entstehen Inkonsistenzen zwischen der freigegebenen und der auf die PU1 transportierten Eigenentwicklung.

Die im IKS-Bereich Ordnungsmäßigkeit definierten Regelungen zur

- Nachvollziehbarkeit,
- Anwendungsentwicklung,
- Transportsystem und zur
- Vornahme von Systemeinstellungen durch das BRZ

sollen diesen Risiken entgegenwirken.

2.2.1 Nachvollziehbarkeit

2.2.1.1 Tabellenprotokollierung

Im Produktivsystem muss die Tabellenprotokollierung aktiviert sein. Es sind alle von SAP standardmäßig vorgesehenen Tabellen zu protokollieren. Der SAP-Hinweis 112388 - Protokollierungspflichtige Tabellen ist entsprechend zu berücksichtigen. Im Transportmanagement sind alle Transporte zu protokollieren.[9] Die Verantwortung für die Durchführung der Tabellen- und Transportprotokollierung liegt gemäß Betriebsvertrag beim BRZ.

Die Umsetzung im SAP-System ist von den Betriebskoordinator:innen in halbjährlichen Abständen zu prüfen.

[9] vgl. BRZ UNISAP-Sicherheitskonzept V7.71, Seite 22 (Dieses liegt bei den SAP-Betriebskoordinator:innen auf. Das Sicherheitskonzept wird aufgrund von Vertraulichkeitserfordernissen dieser Richtlinie nicht beigelegt.)

2.2.1.2 Dokumentation des Anlegens und Löschens von SAP-Benutzer:innenstammsätzen sowie der Rollenzuordnungen

Die Anträge zu den Administrationstätigkeiten in der Benutzer:innen- und Berechtigungsverwaltung müssen aufbewahrt werden, damit die Nachvollziehbarkeit von Änderungen gewährleistet ist. Hierbei ist die gesetzliche Aufbewahrungsfrist zu beachten. Durch die Aufbewahrung der Anträge wird das Risiko vermieden, dass SAP-Benutzer:innen unberechtigt im System angelegt werden oder unberechtigt Rollen an SAP-Benutzer:innen vergeben werden.

2.2.1.3 Namenskonvention für den SAP-Benutzerstammsatz

Als Benutzerkennung ist ein Benutzername zu generieren, der folgendem Muster entspricht: B_NACHNAME. Der Benutzername ist maximal 12 Zeichen lang. Um die Nachvollziehbarkeit sicherzustellen, sind auch die Adressdaten (Vorname, Nachname, E-Mailadresse) im SAP-Benutzerstammsatz zu pflegen. Dies ist für die Nachvollziehbarkeit von Systemaktivitäten notwendig, die von Benutzer:innen mit gleichem Vor- und Nachnamen durchgeführt wurden.
SAP-Zugänge für Mitarbeiter:innen von Beratungsfirmen und sonstigen externen Stellen sind nach folgender Namenskonvention: B_EXT_*NACHNAME* einzurichten.

2.2.1.4 Unzulässigkeit von Sammelbenutzern

Jede Aktion im SAP-System muss eindeutig einer Person zugeordnet werden können. Daher muss es eine 1:1-Beziehung zwischen SAP-Benutzerkennung und einer physischen Person geben. Sammelbenutzer sind daher nicht zulässig. Von dieser Richtlinie ausgenommen sind nur die SAP-Standardbenutzer sowie der Notfallbenutzer. Die Verantwortung für die Dokumentation des Einsatzes dieser Benutzer liegt beim BRZ. [10]

Die Weitergabe des Passworts für den SAP-Zugang ist ebenfalls nicht zulässig, da bei einer Passwort-Weitergabe nicht mehr eindeutig nachvollzogen werden kann, wer mit dieser Benutzerkennung im System gearbeitet hat.

2.2.2 Anwendungsentwicklung

2.2.2.1 Anforderung einer Eigenentwicklung – Interner Change Request (ICR)[11]

Die Anforderung einer Eigenentwicklung muss mittels (elektronischen) Formular zur Beantragung eines Internen Change Requests (ICR) erfolgen. Anforderungsberechtigt ist jede/r Professional User:in. Das Formular für den ICR muss eine detaillierte Definition der Anforderungen enthalten. Nach der Beantragung eines ICR wird dieser von der/dem organisatorischen oder technischen Betriebskoordinator:in überprüft und bei positiver Prüfung ein Umsetzungsvorschlag inkl. Pflichtenheft erstellt. Im Umsetzungsvorschlag wird festgelegt, ob die Umsetzung des ICR intern erfolgt oder extern beauftragt wird. Vor Beginn der Umsetzung wird der ICR-Antrag von der/dem Applikationsverantwortlichen genehmigt. Nach erfolgter Durchführung des ICR, unabhängig davon, ob die Umsetzung intern oder extern erfolgte, muss dieser durch den/die Antragsteller:innen abgenommen werden.

---

[10] vgl. BRZ UNISAP Berechtigungskonzept V2.2, Seite 13 (Dieses liegt bei den SAP-Betriebskoordinator:innen auf. Das Sicherheitskonzept wird aufgrund von Vertraulichkeitserfordernissen dieser Richtlinie nicht beigelegt.)
[11] vgl. Anhang, Kapitel 5.2.2.8: Prozess IKS8 – Abwicklung Interner Change Request (ICR)

2.2.2.2 Freigabeverfahren für Eigenentwicklungen

Anwendungsentwicklung darf ausschließlich im Entwicklungssystem TU1 durchgeführt werden. Nach einem ersten funktionalen Test im Entwicklungssystem wird die Eigenentwicklung auf das Qualitätssicherungssystem QU1 transportiert und durch die jeweils fachlich zuständige Abteilung getestet. Änderungen an der Eigenentwicklung, die aufgrund dieser Tests notwendig werden, dürfen nur auf TU1 vorgenommen werden, anschließend ist die Eigenentwicklung wieder zum Testen nach QU1 zu transportieren. Erst nach der Freigabe durch den/die Antragsteller:in wird die Entwicklung auf das Produktivsystem PU1 transportiert. Sollten bei einer Eigenentwicklung Objekte geändert werden müssen, die im SAP-Namensraum liegen, so ist dies ausführlich zu dokumentieren.

Die Transporte werden vom BRZ durchgeführt. Die Abwicklung und Dokumentation der Transporte erfolgt über das SLF-System.

2.2.2.3 Sperrkonzept

Der Sperrmechanismus wird nicht automatisch vom SAP-System bei jedem ändernden Zugriff auf einen Datensatz aktiviert, sondern muss explizit programmiert werden. In jedem eigenentwickelten Programm, das ändernd auf SAP-Daten zugreift, muss daher von dem/der Entwickler:in dafür gesorgt werden, dass keine Inkonsistenzen entstehen.

2.2.2.4 Berechtigungsprüfungen

In eigenentwickelten Programmen müssen Berechtigungsprüfungen implementiert werden. Wenn die Berechtigungsprüfung nicht explizit programmiert wurde, kann das Programm von jedem/r SAP-Benutzer:in ausgeführt werden. Die relevanten Berechtigungsprüfungen sind in den Programmiervorgaben festzulegen.

2.2.2.5 Dokumentation

Jedes Programm ist ausführlich zu dokumentieren. Die Dokumentation muss aus einer Dokumentation für die Anwender:innen und einer technischen Dokumentation für andere Entwickler:innen bestehen.

2.2.2.6 Direkter Datenbankzugriff

Zugriffe auf die Datenbank dürfen grundsätzlich nur über das Data Dictionary stattfinden. Der direkte Datenbankzugriff unter Umgehung der R/3 Datenbankschnittstelle darf in Anwendungsprogrammen nicht verwendet werden, da dadurch die Sicherheit und Konsistenz der Daten nicht gewährleistet ist.

2.2.2.7 Versionierung

Alle Versionen von Programmen sind aufbewahrungspflichtig. Das Löschen der Versionshistorie ist nicht zulässig. Die Aufbewahrungspflicht wird auch erfüllt, wenn die Versionen von eigenentwickelten Programmen im Entwicklungssystem archiviert werden.

2.2.2.8 Datenänderungen im Debug-Modus

Änderungen von Hauptspeicherinhalten im Debug-Modus werden nicht protokolliert. Da im Debug-Modus jedoch betriebswirtschaftliche Werte während des Ablaufs eines Programms verändert werden können, darf dieses Zugriffsrecht im Produktivsystem niemandem zugeordnet werden.

2.2.3 Transportsystem

Um zu verhindern, dass Entwickler:innen ihre Eigenentwicklungen ohne Freigabeverfahren ins Produktivsystem transportieren können, ist eine Funktionstrennung zwischen Entwicklung und Transporten zu realisieren. Daraus folgt, dass die Berechtigungen für die Entwicklung und das Transportsystem nicht gemeinsam an eine Person der Univerität Graz vergeben werden dürfen. Da die Trennung der Berechtigungen für die Entwicklung und den Transport bei Mitarbeiter:innen des BRZ aus organisatorischen Gründen nicht möglich ist, wurde vom BRZ technisch sichergestellt, dass die/der Entwickler:in die eigenen Entwicklungen nicht transportieren kann.

2.2.4 Vornahme von Systemeinstellungen durch das BRZ

Die Universität ist von sämtlichen geplanten Eingriffen in das System zu informieren. Dies gilt insbesondere für Customizing-Einstellungen und Entwicklungen. Die durchgeführten Tätigkeiten sind vom BRZ zu dokumentieren und den Betriebskoordinator:innen der Universität zur Verfügung zu stellen.

Von den Betriebskoordinator:innen ist anhand der im SLA-Report angeführten Transporte monatlich zu prüfen, welche vom BRZ am Mandanten der Univerität Graz durchgeführten Eingriffe (Customizing-Einstellungen und Entwicklungen) transportiert wurden.

2.3 IKS-Bereich: Wirtschaftlichkeit

Im IKS-Bereich Wirtschaftlichkeit kann insbesondere folgendes Risiko auftreten:

- **Bezahlung zu hoher Lizenzkosten**
  Zu hohe Lizenzkosten können anfallen, wenn seitens des BRZ fehlerhafte Lizenzverrechnungen erfolgen oder seitens der Universität gegen Lizenzbestimmungen verstoßen wird.

Die im IKS-Bereich Sicherheit definierten Regelungen zur

- Verrechnung von Lizenzkosten,
- Einhaltung der SAP-Lizenzbestimmungen,
- Vergabe von Nutzertypen und zum
- Lizenzvolumen

sollen dem Eintreten dieses Risikos entgegenwirken.

2.3.1 Verrechnung von Lizenzkosten

Die vom BRZ in Rechnung gestellten Lizenzgebühren werden von den Betriebskoordinator:innen geprüft.

Die Modalitäten eventueller Weiterverrechnungen sind in gesonderten Regelungen enthalten.

2.3.2 Einhaltung der SAP-Lizenzbestimmungen

Mehrfachanmeldungen im Produktivsystem verstoßen gegen das Lizenzabkommen mit SAP und sind daher technisch deaktiviert.

2.3.3 Lizenzvolumen

Von SAP wird in regelmäßigen Abständen eine Systemvermessung in Abstimmung mit dem BRZ durchgeführt. Im Zuge der Lizenzvermessung sind von der Benutzer:innen- und Berechtigungsverwaltung die, der Lizenzverrechnung zugrunde liegenden Zahlen an das BRZ zu melden. Sollte das Lizenzvolumen überschritten werden, ist das weitere Vorgehen zu klären, da in diesem Fall Lizenzen nachzukaufen sind.

3 Nicht-Produktivsysteme

3.1 Qualitätssicherungssystem (QU1-102)

Im Qualitätssicherungssystem finden die Produktionsvorbereitung sowie die Abnahme von Entwicklungen aus dem Entwicklungssystem statt. Das QU1-System ist an der Universität Graz einer gesondert definierten Gruppe von Benutzer:innen zugänglich, die für die Weiterentwicklung und Optimierung des SAP-Systems verantwortlich ist. Für diese Arbeiten sind umfangreiche Berechtigungen notwendig.

Die Vergabe der Berechtigungen erfolgt durch die Benutzer:innen- und Berechtigungsverwaltung.

3.2 Entwicklungssystem (TU1)

Das Entwicklungssystem ist der Ausgangspunkt für Eigenentwicklungen und alle Customizing-Einstellungen. Hinsichtlich der Berechtigungen und der Zugangsbestimmungen gelten die gleichen Regelungen wie für das Qualitätssicherungssystem, da auf TU1 erste funktionale Tests durchgeführt werden müssen.

Die Vergabe der Berechtigungen erfolgt durch das Betriebskoordinatorenteam.

3.3 Schulungsmandant (QU1-502)

Das Schulungssystem steht allen Anwender:innen zur Verfügung. Da der Schulungsmandant eine Kopie des Produktivsystems ist, müssen die Berechtigungen am Schulungsmandanten den Berechtigungen auf dem Produktivsystem entsprechen.

Die Vergabe der Berechtigungen erfolgt durch die Benutzer:innen- und Berechtigungsverwaltung.

4 Ausgelagerte Bereiche des SAP-Systems

4.1 ERP-System

Der Betrieb der SAP-Basiskomponenten ist an das BRZ ausgelagert. Das BRZ ist dafür verantwortlich, dass der Betrieb der ausgelagerten Bereiche den Anforderungen einer Revision bzw. Wirtschaftsprüfung entspricht.

Das Sicherheitskonzept des BRZ liegt bei den SAP-Betriebskoordinator:innen auf.

Der Nachweis der Zertifizierung des Sicherheitsmanagements des BRZ gem. ISO 27001 liegt dieser Richtlinie bei.[12]

4.2 SAP Business Warehouse (SAP BW)

Neben dem SAP ERP wird von der Universität auch noch ein SAP Business Warehouse eingesetzt. Das SAP Business Warehouse der Universität wird von der Axians ICT Austria GmbH betrieben.

Die in den vorangegangenen Kapiteln dieser Richtlinie enthaltenen Regelungen gelten mit Ausnahme der im Folgenden angeführten Punkte auch für das SAP Business Warehouse.

Tätigkeiten, die für das SAP ERP lt. dieser Richtlinie vom BRZ durchgeführt werden, werden für das SAP Business Warehouse durch die Axians ICT Austria GmbH durchgeführt.

Die Nachweise der Zertifizierung der Axians ICT Austria GmbH gem. ISO 27001 liegt dieser Richtlinie bei[13]. Der Report gem. SAS70 bzw. ISAE3402 liegt bei den SAP-Betriebskoordinator:innen auf.

4.2.1 Für das SAP BW nicht relevante Regelungen dieser Richtlinie

Kapitel	Seite	Begründung
2.2.1.1 Tabellenprotokollierung	16	Der SAP Hinweis 112388 bezieht sich auf Tabellen des ERP und nicht auf das BW; für das BW gibt es keine entsprechenden Protokollierungsrichtlinien

[12] vgl. Anhang Kapitel 5.4: Sicherheitszertifikat gem. ISO 27001 (BRZ)
[13] vgl. Anhang Kapitel 5.5: Sicherheitszertifikat gem. ISO 27001 und SAS70 bzw. ISAE3402 (Axians ICT Austria GmbH)

4.2.2 Für das SAP BW in geänderter Form relevante Regelungen

Kapitel	Seite	Begründung
2.1.2.3 Kennwortregelung	11	Bei der Vergabe des Initialkennwortes in SAP BW ist nach denselben Regeln wie in Kapitel 2.1.2.3 angeführt, vorzugehen. Falls der BW-Zugang gleichzeitig mit dem ERP-Zugang angelegt wird, ist als Initialpasswort in SAP BW der gleiche PIN wie für den SAP-Zugang zu verwenden.
2.2.1.3 Namenskonvention für den SAP-Benutzerstammsatz	17	Der Benutzername im BW lautet gleich wie jener für den SAP-Zugang.
2.2.2.1 Anforderung einer Eigenentwicklung	17	Zu den Eigenentwicklungen zählen im SAP BW auch Änderungen am Datenmodell und an Objekten des BW (zB InfoAreas, InfoPackages, InfoSources, DataStoreObjects und Infocubes) sowie die Änderung von Prozessketten
2.2.2.2 Freigabeverfahren für Eigenentwicklungen	18	Entwicklungs- und Qualitätssicherungssystem sind in der BW-Systemlandschaft zu einem System zusammengefasst. Daher erfolgen alle Tests für den Freigabeprozess auf dem BW-Entwicklungssystem. Die Transporte für die Produktivsetzung der Eigenentwicklung werden von der Axians durchgeführt, sobald der Auftrag im Transportmanagement freigegeben wurde.
2.2.2.4 Berechtigungsprüfungen	18	Falls BW-Queries Benutzer:innen ohne Gesamtberechtigung auf alle CO-Kontierungen der Universität zur Verfügung gestellt werden, ist entweder beim Erstellen der Query selbst oder durch geeignete Berechtigungsvergabe in den Rollen (zB mittels Analyseobjekten) sicherzustellen, dass nur Daten von CO-Kontierungen eingesehen werden können, für die der bzw. die BW-Benutzer:in berechtigt sind.

4.2.3 Für das SAP BW zusätzlich geltende Regelungen

Kapitel	Seite	Begründung
Entwicklungs- und Qualitätssicherungssystem SAP BW	22	Die BW-Systemlandschaft ist zweistufig aufgebaut. Entwicklungs- und Qualitätssicherungssystem sind zu einem System zusammengefasst. Für das BW-Entwicklungssystem gelten dieselben Regelungen wie für das Entwicklungs- und Qualitätssicherungssystem des ERP.

Der Rektor:
Riedler

5 Anhang

5.1 Zusammenfassung der Verantwortlichkeiten aus der IKS-Richtlinie

Die sich aus dieser Richtlinie ergebenden Verantwortlichkeiten sind in der folgenden Matrix nochmals zusammengefasst.

5.1.1 Benutzer:innen- und Berechtigungsverwaltung, SAP-Betriebskoordination, Applikationsverantwortliche/r

IKS-Bereich		Richtlinie	Benutzer:innen- und Berechtigungsverwaltung	SAP-Betriebskoordination	Applikationsverantwortliche/r
2 Produktivsystem (PU1)					
2.1 Sicherheit					
	2.1.1 Netzwerksicherheit	Seite 8f		➢ Überprüfung des Vorhandenseins einer gesicherten Verbindung Uni <=> BRZ	
	2.1.2 Anmeldesicherheit	Seite 9ff	➢ Vergabe des PINs ➢ Anlegen, Sperren, Freischalten, Löschen von SAP-Zugängen ➢ Überprüfung der Umsetzung im System i.S.d. Vier-Augen-Prinzips	➢ Prüfung der SAP-Professional User-Anträge auf Vereinbarkeit mit den IKS-Regelungen ➢ Prüfung der Einhaltung der in der Richtlinie festgelegten Namenskonventionen und Rollenzuordnungen für Mitarbeiter:innen des BRZ ➢ Prüfung, ob von Mitarbeiter:innen des BRZ schreibende Zugriffe auf Applikationsdaten vorgenommen wurden (monatlich)	➢ Genehmigung von SAP-Professional User-Anträgen
	2.1.3 Berechtigungsverwaltung	Seite 13ff	➢ Technische Umsetzung Berechtigungskonzept; ➢ Vergabe von Rollen an Benutzer:innen ➢ technische Umsetzung Rollenänderungen ➢ Überprüfung der Umsetzung im System i.S.d. Vier-Augen-Prinzips	➢ Berücksichtigung von kritischen Berechtigungen ➢ Erstellung der Information der Rollenzuordnung für Professional User:innen	➢ Genehmigung von Berechtigungsänderungen bei Professional User:innen

IKS-Bereich		Richtlinie	Benutzer:innen- und Berechtigungsverwaltung	SAP-Betriebskoordination	Applikationsverantwortliche/r
2.2 Ordnungsmäßigkeit					
	2.2.1 Nachvollziehbarkeit	Seite 16f	➢ Dokumentation der Administrationstätigkeiten; ➢ Einhaltung der Namenskonvention	➢ Prüfung der Einstellungen zu protokollierungspflichtigen Tabellen (halbjährlich)	
	2.2.2. Anwendungsentwicklung	Seite 17f		➢ Prüfung von ICRs; ➢ Erarbeitung von Umsetzungsvorschlägen für ICRs	➢ Genehmigung von ICRs
	2.2.3 Transportsystem	Seite 19	➢ Rollenmäßige Trennung zwischen Entwicklungs- und Transportberechtigung		
	2.2.4 Systemeinstellungen durch das BRZ	Seite 19		➢ Prüfung, welche vom BRZ durchgeführten Eingriffe transportiert wurden	
2.3 Wirtschaftlichkeit					
	2.3.1 Verrechnung von Lizenzkosten	Seite 20		➢ Prüfung, der vom BRZ in Rechnung gestellten Lizenzkosten	
	2.3.2 Einhaltung der SAP-Lizenzbestimmungen	Seite 20			
	2.3.3 Lizenzvolumen	Seite 20	➢ Klärung des Vorgehens bei Überschreitung des Lizenzvolumens		
3 Nicht-Produktivsysteme					
3.1 Qualitätssicherungssystem (QU1-102)		Seite 21	➢ Vergabe von Berechtigungen für QU1-102		
3.2 Entwicklungssystem (TU1)		Seite 21		➢ Vergabe von Berechtigungen für TU1	
3.3 Schulungsmandant (QU1-502)		Seite 21	➢ Vergabe von Berechtigungen für QU1-502		

5.1.2 uniIT, BRZ, SAP-Betriebskoordination, Benutzer:innen- und Berechtigungsverwaltung

IKS-Bereich		Richtlinie	uniIT	BRZ	SAP-Betriebskoordination	Benutzer:innen- und Berechtigungsverwaltung
2 Produktivsystem (PU1)						
2.1 Sicherheit						
	2.1.1 Netzwerksicherheit	Seite 8f	➢ Inhalt und Umsetzung Security Policy	➢ Herstellung einer gesicherten Verbindung Uni <=> BRZ	➢ Überprüfung des Vorhandenseins einer gesicherten Verbindung Uni <=> BRZ (wöchentlich)	
	2.1.2 Anmeldesicherheit	Seite 9ff		➢ Verwaltung der SAP-Zugänge von CCC-Mitarbeiter:innen ➢ Informieren der Uni, wenn wesentliche Veränderungen an den Berechtigungen von Mitarbeiter:innen des BRZ vorgenommen werden	➢ Prüfung der Einhaltung der in der Richtlinie festgelegten Namenskonventionen und Rollenzuordnungen für Mitarbeiter:innen des BRZ (monatlich) ➢ Prüfung, ob von Mitarbeiter:innen des BRZ schreibende Zugriffe auf Applikationsdaten vorgenommen wurden (monatlich)	
	2.1.3 Berechtigungsverwaltung	Seite 13ff				
2.2 Ordnungsmäßigkeit						
	2.2.1 Nachvollziehbarkeit	Seite 16f		➢ Tabellen- und Transportprotokollierung	➢ Prüfung der Einstellungen zu protokollierungspflichtigen Tabellen (halbjährlich)	
	2.2.2. Anwendungsentwicklung	Seite 17f		➢ Transporte der Eigen-entwicklungen durchführen		
	2.2.3 Transportsystem	Seite 19				
	2.2.4 Systemeinstellungen durch das BRZ	Seite 19		➢ Weitergabe detaillierter Informationen über geplante und vorgenommene Systemeinstellungen	➢ Prüfung, welche vom BRZ durchgeführten Eingriffe transportiert wurden (monatlich)	

IKS-Bereich	Richtlinie	unilT	BRZ	SAP-Betriebskoordination	Benutzer:innen- und Berechtigungsverwaltung
2.3 Wirtschaftlichkeit					
2.3.1 Verrechnung von Lizenzkosten	Seite 20		➢ Verrechnung der Lizenzgebühren	➢ Prüfung, der vom BRZ in Rechnung gestellten Lizenzkosten	
2.3.2 Einhaltung der SAP-Lizenzbestimmungen	Seite 20				
2.3.3 Lizenzvolumen	Seite 20				➢ Klärung des Vorgehens bei Überschreitung des Lizenzvolumens
3 Nicht-Produktivsysteme					
3.1 Qualitätssicherungssystem (QU1-102)	Seite 21				➢ Vergabe von Berechtigungen für QU1-102
3.2 Entwicklungssystem (TU1)	Seite 21			➢ Vergabe von Berechtigungen für TU1	
3.3 Schulungsmandant (QU1-502)	Seite 21				➢ Vergabe von Berechtigungen für QU1-502
4 Ausgelagerte Bereiche des SAP-Systems	Seite 22		➢ Betrieb der SAP-Basiskomponenten, der den Anforderungen einer Revision bzw. Wirtschaftsprüfung entspricht		

5.2 Geschäftsprozesse, die sich aus der IKS-Richtlinie ergeben

Die sich aus der Richtlinie ergebenden Geschäftsprozesse sind im Folgenden grafisch dargestellt.

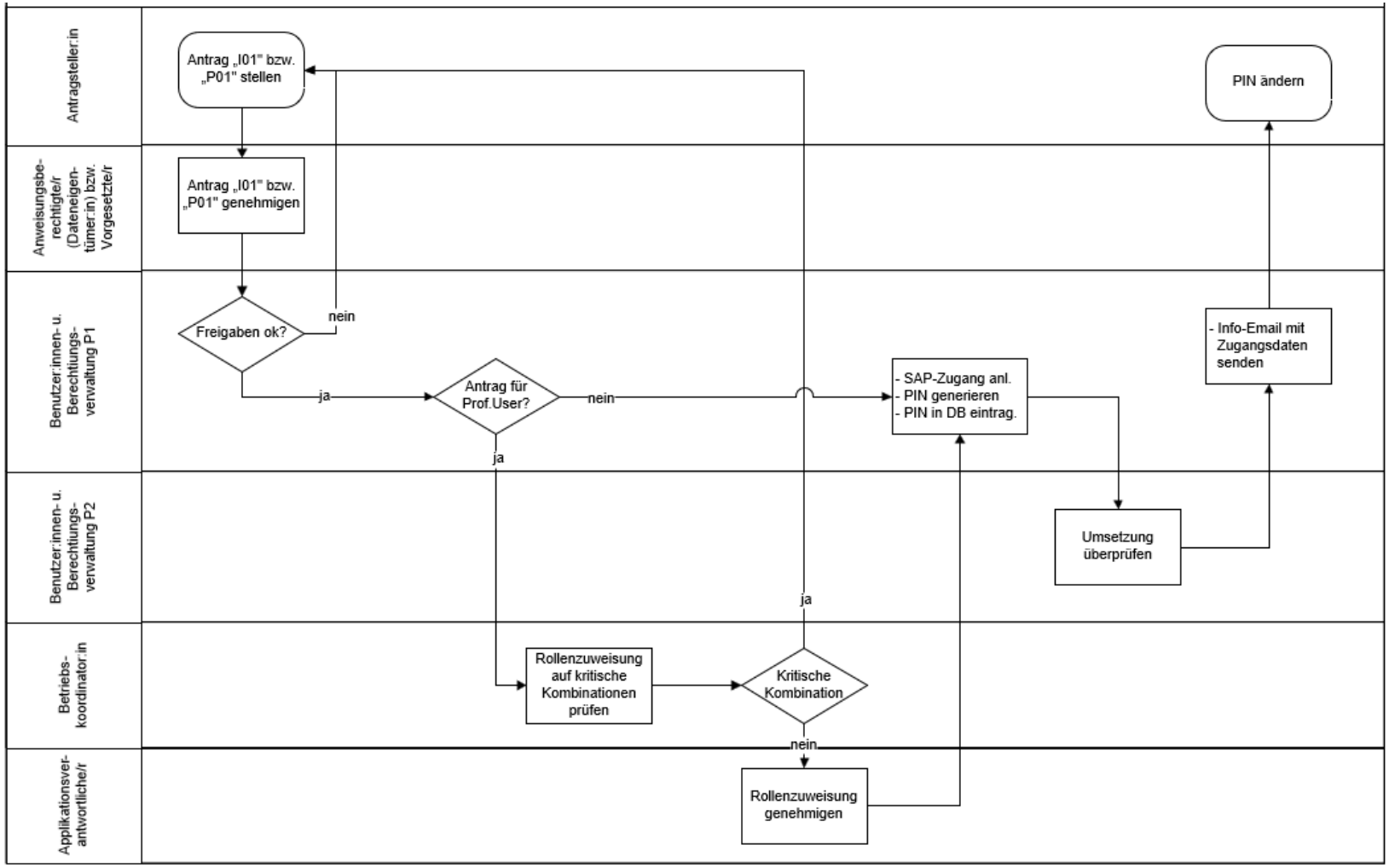
5.2.1 Rollenbeschreibung bzw. –definition

Rolle	Prozess	Beschreibung/Definition
Antragsteller:in	IKS1_Neuer SAP-Zugang IKS3_Passwort zurücksetzen IKS4_Übertragung eines SAP-Zuganges	Jede/r Mitarbeiter:in der KFUG, die/der im Rahmen ihrer/seiner Arbeit einen SAP-Zugang benötigt bzw. auf die/den eine SAP-Lizenz übertragen werden soll
SAP-User:in	IKS3_Passwort zurücksetzen IKS4_Sperren, Freischalten, Löschen eines SAP-Zugangs IKS6_Berechtigungsänderung	Jede/r SAP-User:in der KFUG
SAP Prof.	IKS7_Rollenänderung IKS8_Abwicklung ICR	Jede/r SAP Prof. User:in der KFUG
Anweisungsberechtigte/r + (Dateneigentümer:in)	IKS1_Neuer SAP-Zugang IKS4_Sperren, Freischalten, Löschen eines SAP-Zugangs IKS5_Übertragung eines SAP-Zuganges IKS6_Berechtigungsänderung	Dateneigentümer:innen sind die Anweisungsberechtigten des Berechtigungsobjektes, auf die der neue SAP-Zugang berechtigt ist.
Vorgesetzte/r	IKS6_Berechtigungsänderung IKS7_Rollenänderung	Vorgesetzte/r der/des SAP-Userin/s
Benutzer:innen- und Berechtigungsverwaltung	IKS1_Neuer SAP-Zugang IKS2_Neuer ESS-Zugang IKS3_Passwort zurücksetzen IKS4_Sperren, Freischalten, Löschen eines SAP-Zuganges IKS5_Übertragung eines SAP-Zuganges IKS6_Berechtigungsänderung IKS7_Rollenänderung IKS8_Abwicklung ICR	Mitarbeiter:innen des Competence Center SAP der Universität Graz
Betriebskoordinator:in	IKS1_Neuer SAP-Zugang IKS6_Berechtigungsänderung IKS7_Rollenänderung IKS8_Abwicklung ICR	Fr. Hungerländer-Kropf (organisatorisch), Hr. Ortner (technisch)
Applikationsverant-wortliche/r	IKS1_Neuer SAP-Zugang IKS6_Berechtigungsänderung IKS7_Rollenänderung IKS8_Abwicklung ICR	Applikation SAP HR (Hr. Lugger) Applikation SAP FI, FI-AA, CO, MM/SD, BW und VM (Hr. Zettl)
Entwickler:in	IKS8_Abwicklung ICR	Mitarbeiter:innen des Competence Center SAP der Universität Graz
Externe/r Lieferant:in	IKS8_Abwicklung ICR	Jede externe Firma, die in die Umsetzung eines ICR involviert ist
uniIT	IKS2_Neuer ESS-Zugang	Betreuer:in des automatischen Abgleichs der SAP-Zugangsdaten mit den LDAP-Daten

5.2.2 Prozesse

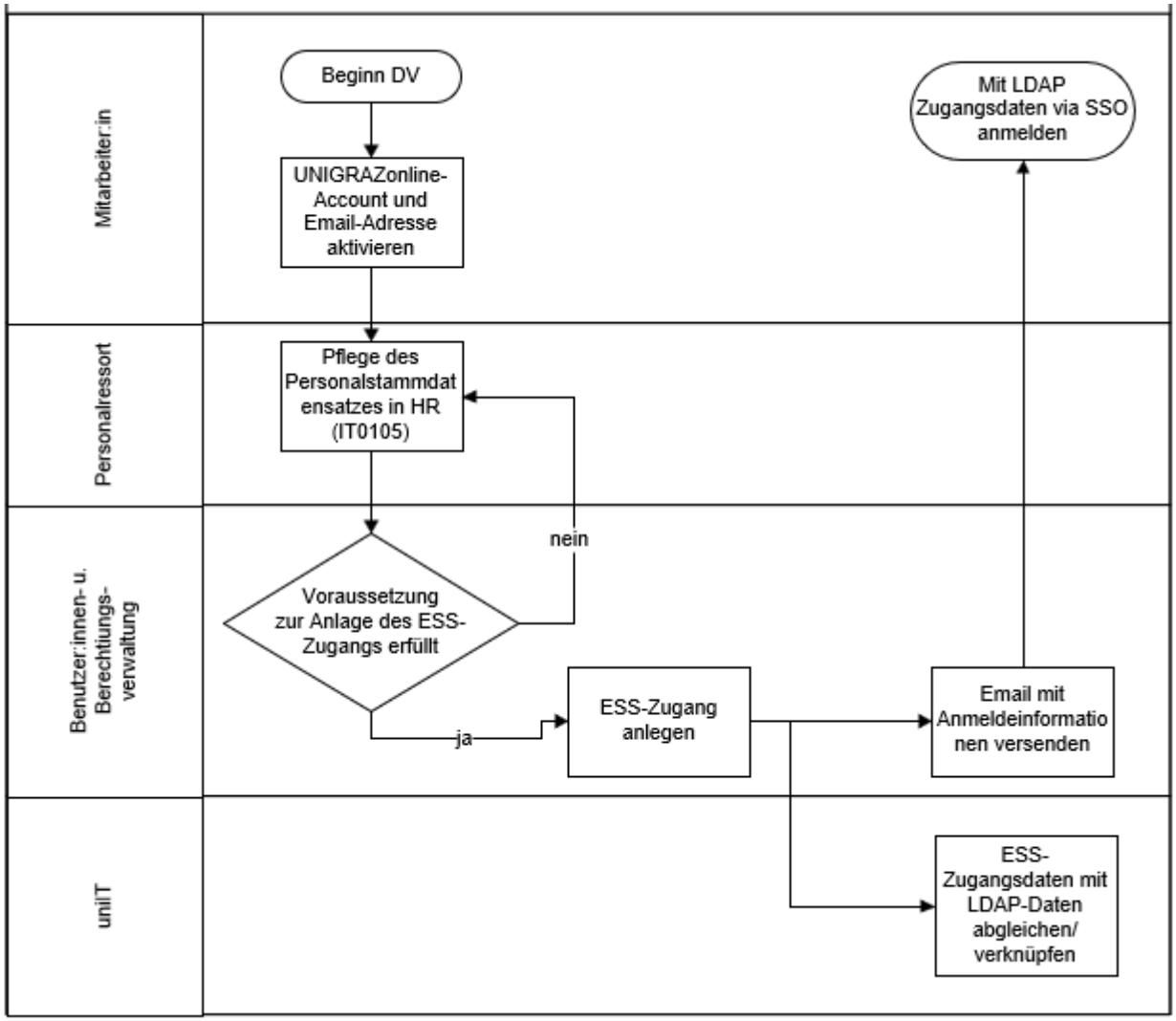
5.2.2.1 Prozess IKS1 – Neuer SAP-Zugang

Dieser Prozess bezieht sich auf Punkt **2.1.2.1** in der Richtlinie.



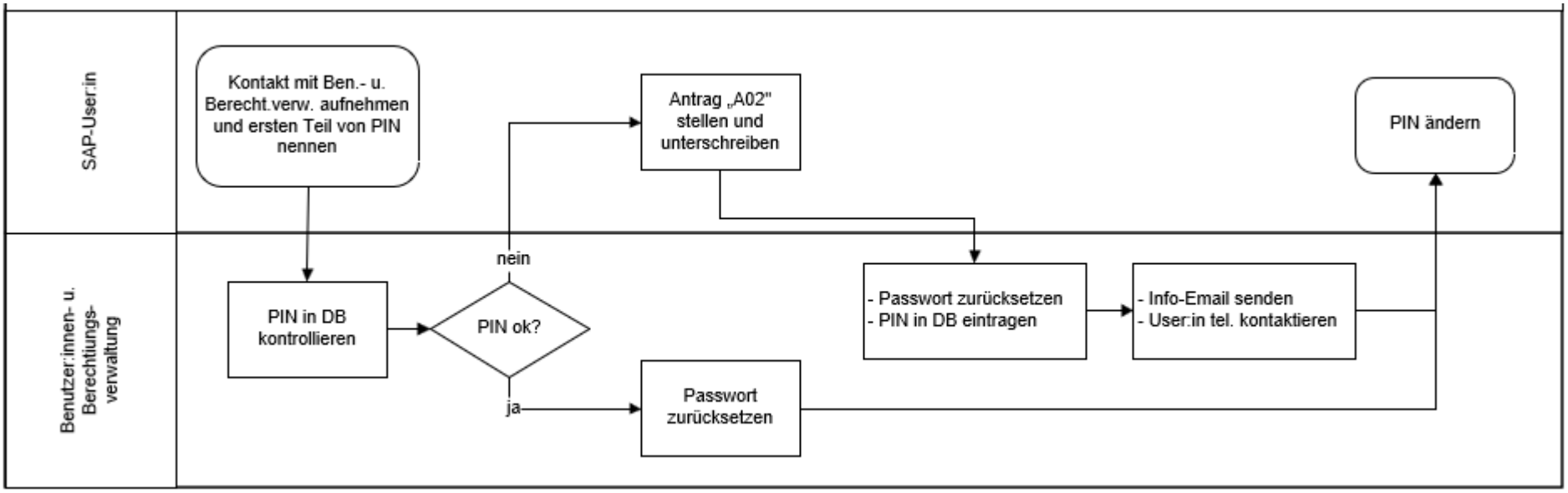
5.2.2.2 Prozess IKS2 – Neuer ESS-Zugang

Dieser Prozess bezieht sich auf Punkt **2.1.2.2** in der Richtlinie.



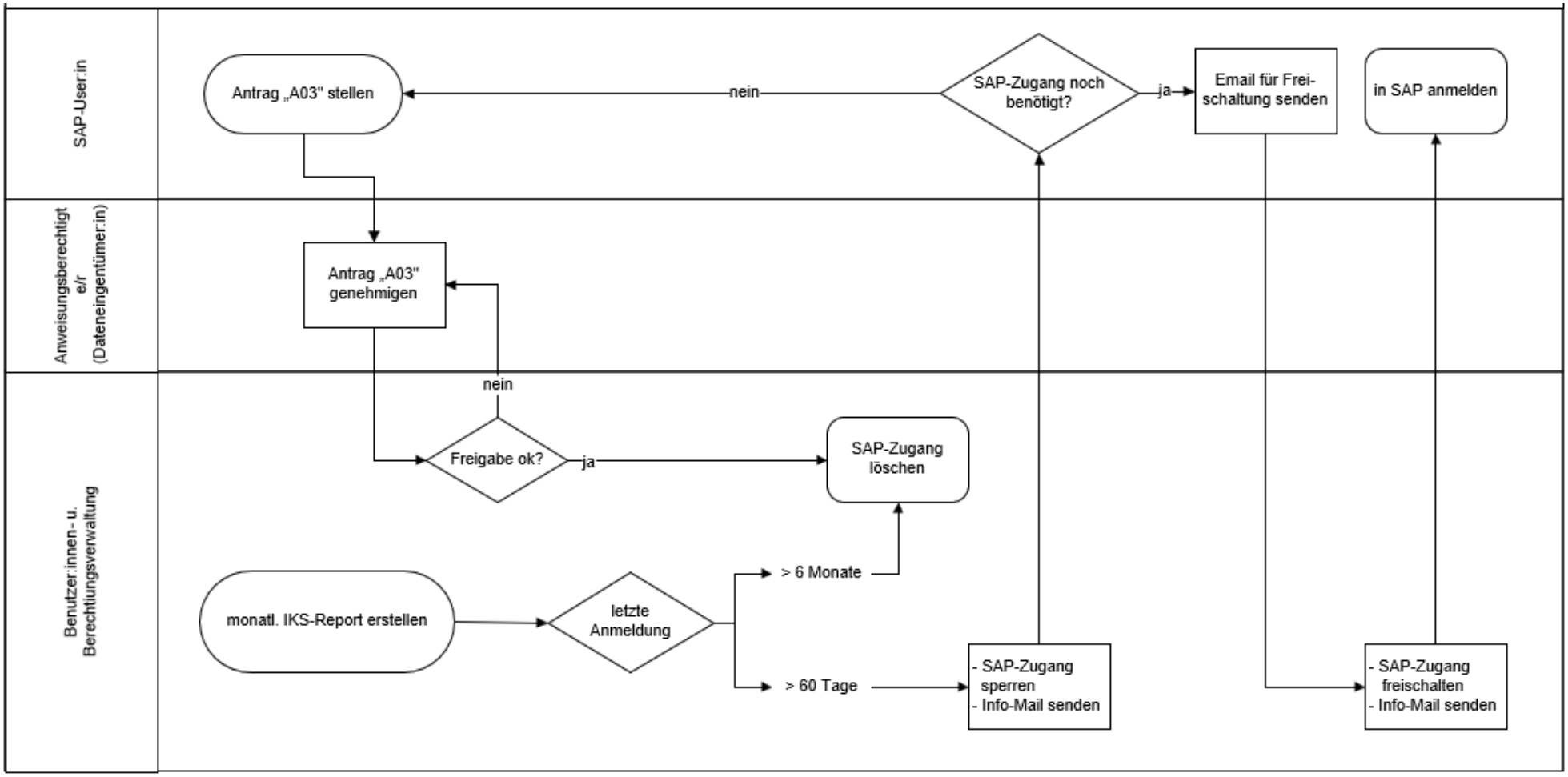
5.2.2.3 Prozess IKS3 - Passwort zurücksetzen

Dieser Prozess bezieht sich auf Punkt **2.1.2.3** in der Richtlinie.



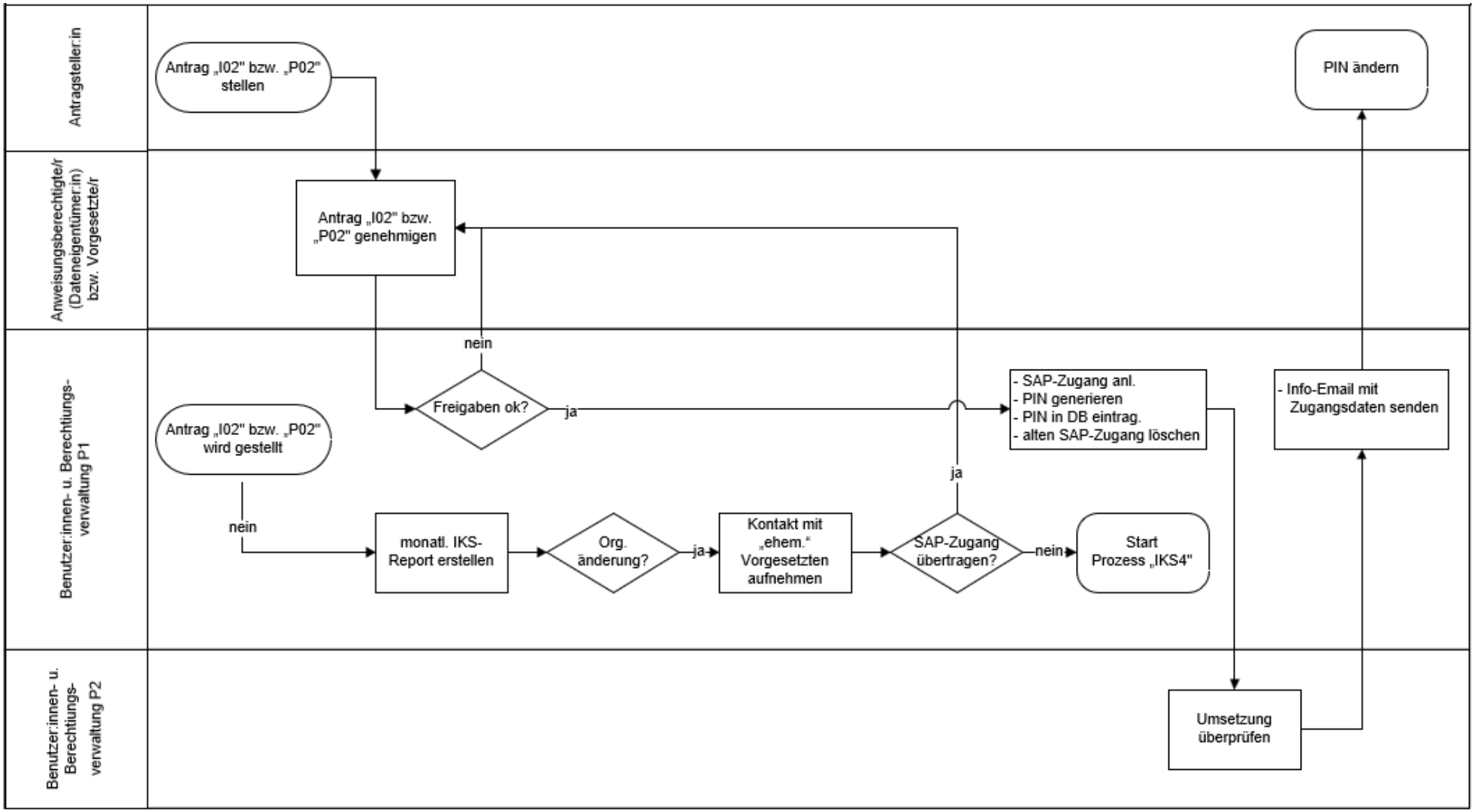
5.2.2.4 Prozess IKS4 - Sperren, Freischalten und Löschen eines SAP-Zugangs

Dieser Prozess bezieht sich auf Punkt **2.1.2.5** der Richtlinie



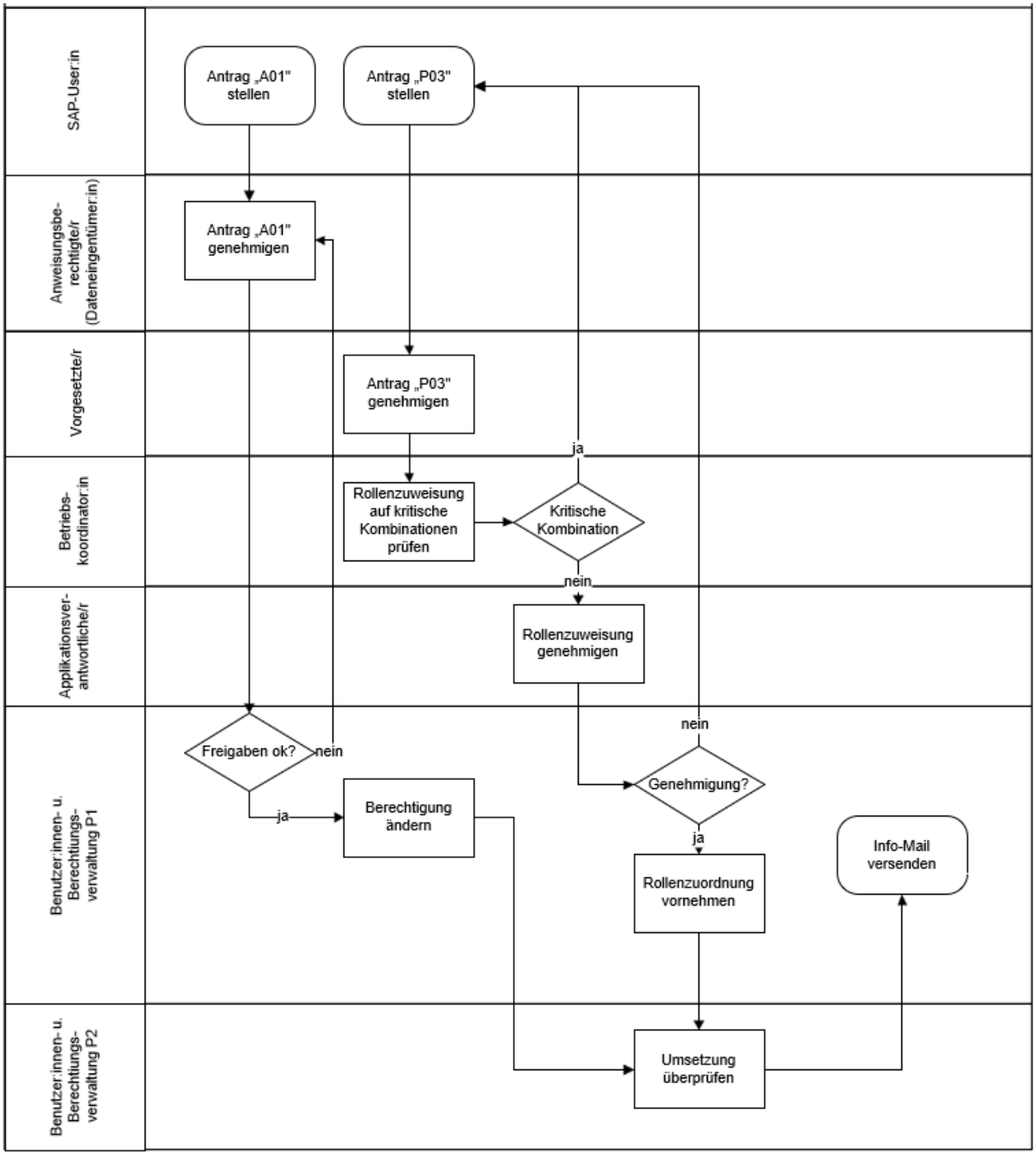
5.2.2.5 Prozess IKS5 - Übertragung eines SAP-Zugangs

Dieser Prozess bezieht sich auf Punkt **2.1.3.1.3** in der Richtlinie.



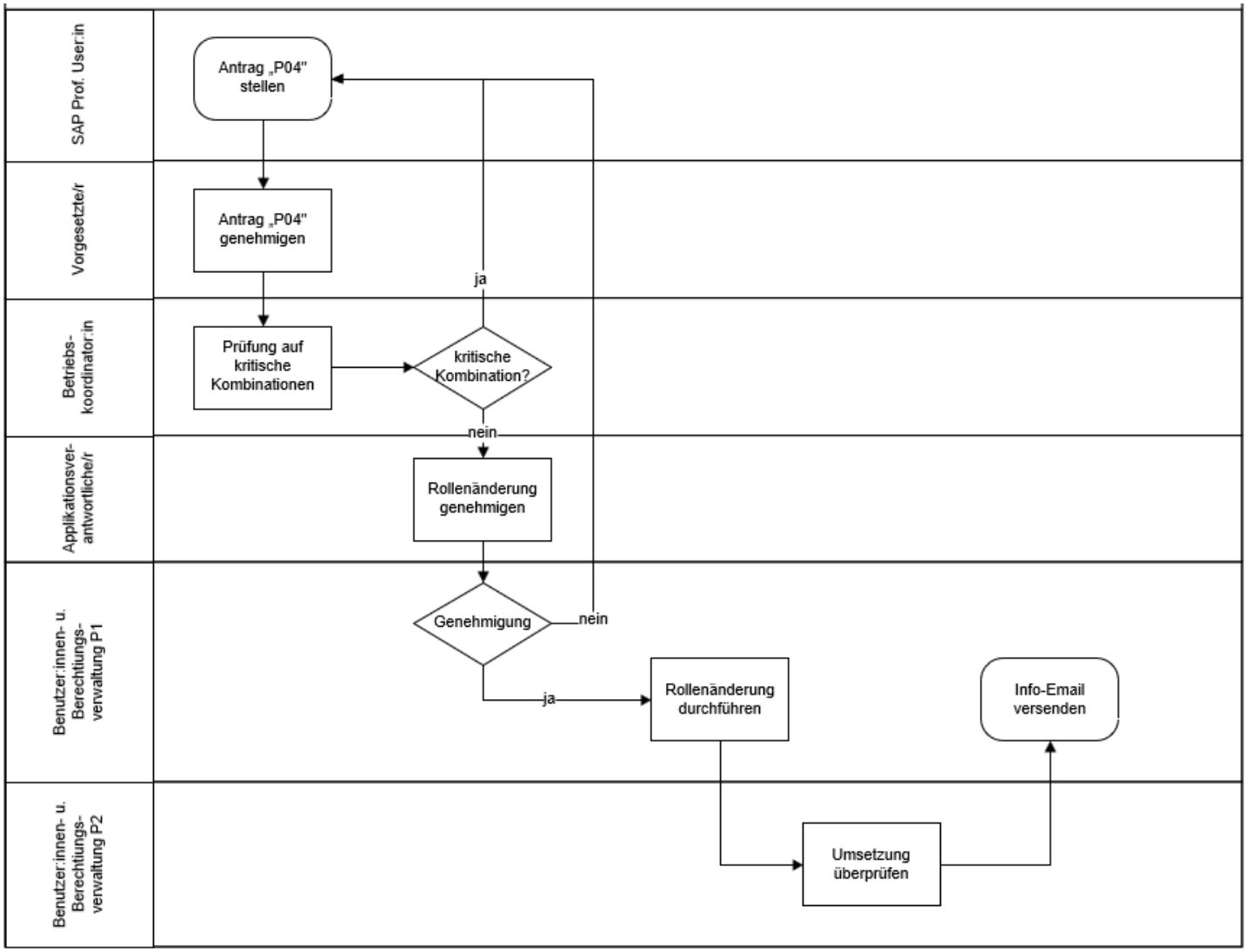
5.2.2.6 Prozess IKS6 - Berechtigungsänderung

Dieser Prozess bezieht sich auf Punkt **2.1.3.1.3** in der Richtlinie.



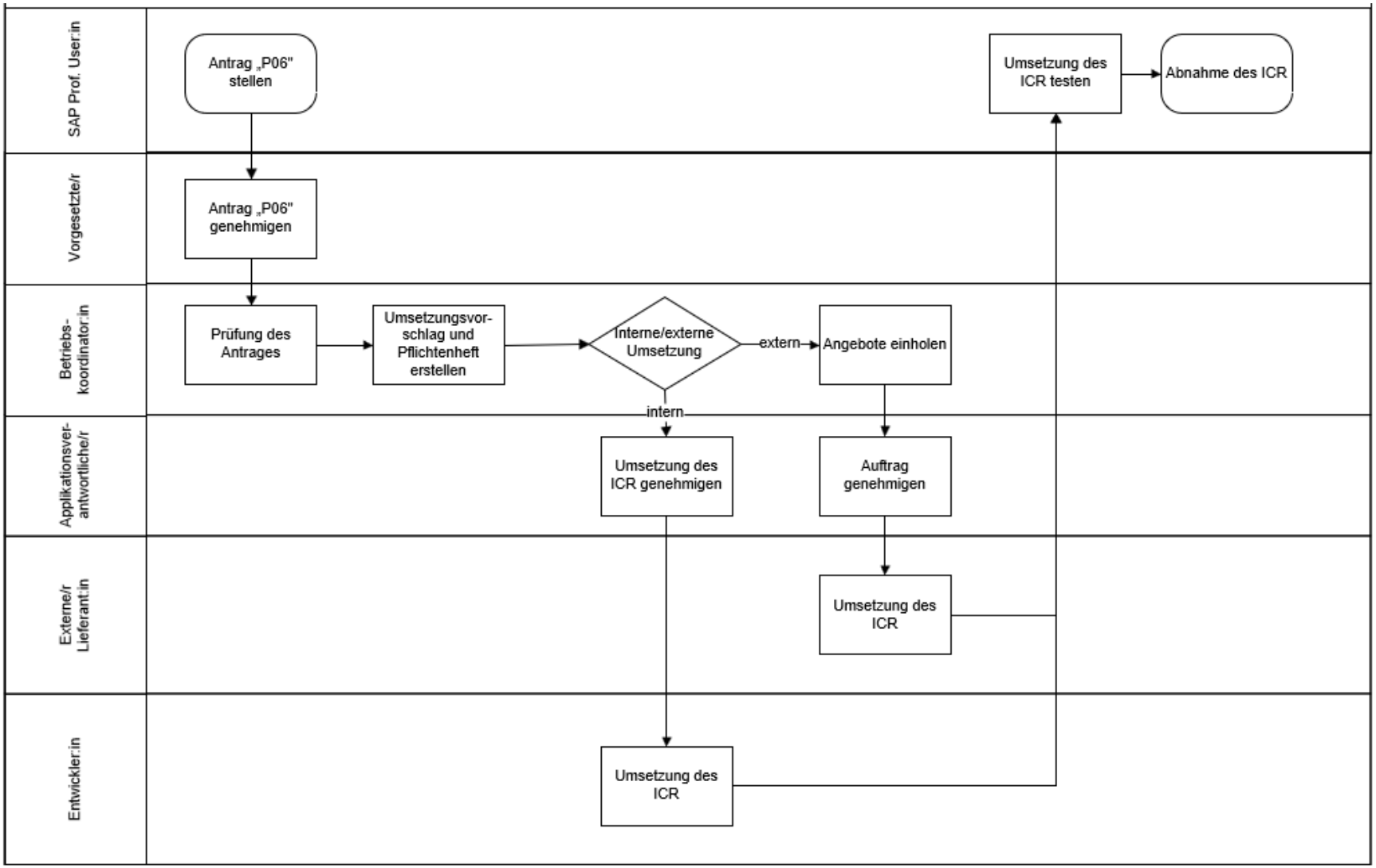
5.2.2.7 Prozess IKS7 – Rollenänderung

Dieser Prozess bezieht sich auf Punkt **2.1.3.1.4** in der Richtlinie.



5.2.2.8 Prozess IKS8 - Abwicklung Interner Change Request (ICR)

Dieser Prozess bezieht sich auf Punkt **2.2.2.1** in der Richtlinie.



5.3 Auszug aus Angebot „VPN-Anbindung“

Seite 9

2.2 Leistungsumfang

Die BRZ GmbH erbringt folgende Leistungen:

- Herstellung der VPN-Anbindung
- Betreuung und Entstörung der Infrastruktur, vom Router (inklusive) an der Universität bis zum UNISAP-Server
- Es gelten die Verfügbarkeitszeiten des definierten SLA mit der Karl-Franzens-Universität Graz; für Pönalisierungen ist allerdings nur die zentrale Messklammer maßgeblich

2.3 Leistungsabgrenzung

Es sind nur jene Leistungen Bestandteil des Angebotes, die unter Punkt 2.2 (Leistungsumfang) abschließend aufgezählt sind.

5.4 Sicherheitszertifikat gem. ISO 27001 (BRZ)

www.cis-cert.com

SECURITY CIS CERTIFICATION® INFORMATION

Zertifikat

Bundesrechenzentrum GmbH
Hintere Zollamtsstraße 4, 1030 Wien

BRZ

Dieses Zertifikat bestätigt, dass die oben genannte Organisation auditiert wurde und ein wirksames

INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM
betreibt entsprechend den Anforderungen der internationalen Norm
ISO/IEC 27001:2013

Geltungsbereich und Anwendbarkeit:
gesamtes Unternehmen

Zertifizierte Standorte/Organisationseinheiten:
Hintere Zollamtsstraße 4, 1030 Wien
Erdbergstraße 186-198, 1030 Wien
Gruberstraße 63, 4020 Linz

Entsprechend dem Statement of Applicability (Statement of Applicability_V4.4.pdf) V4.4 vom 06.04.2023.

Registrier-Nummer: I-00013/0

Erstausstellung: 23.05.2005

Gültig bis: 31.10.2025

Wien, am 16.05.2023

Unterschrift aus Sicherheitsgründen entfernt
DI (FH) Harald Erkinger CEO
CIS - Certification & Information Security Services GmbH

CIS arbeitet im Bereich der Systemzertifizierung nach den Vorgaben des Internationalen Standards ISO 17021 und ist diesbezüglich von der Akkreditierung Austria akkreditiert.

Die Gültigkeit des CIS-Zertifikats wird durch jährliche Überwachungsaudits sichergestellt und muss durch ein Rezertifizierungsaudit nach drei Jahren erneuert werden. Die aktuelle Gültigkeit des Zertifikats ist ausschließlich unter www.cis-cert.com/service/zertifikatssuche/ dokumentiert.

5.5 Sicherheitszertifikat gem. ISO 22301 und ISO 27001 bzw. ISAE3402 (Axians ICT Austria)

Certificate of Registration

nqa.

This is to certify that the Business Continuity Management System of:

Interxion HeadQuaters B.V.
Scorpius 30, 2132 LR Hoofddorp, The Netherlands

(Central function listed above. See appendix for additional locations)

applicable to:

The Business Continuity Management System in relation to the delivery of data centre services.

has been assessed and registered by NQA against the provisions of:

ISO 22301:2019

This registration is subject to the company maintaining a business continuity management system to the above standard, which will be monitored by NQA

Managing Director

Certificate No.	174236
ISO Approval Date:	27 September 2010
Reissued:	23 November 2022
Valid Until:	23 November 2025
EAC Code:	33

UKAS MANAGEMENT SYSTEMS

0015

Der Report gem. ISO 27001 bzw. ISAE3402 liegt bei den SAP-Betriebskoordinator:innen auf.

5.6 Formulare

Alle Formulare, deren Notwendigkeit sich aus den vorhergehenden Kapiteln ergibt, sind unter https://intranet.uni-graz.at/einheiten/SAP/Pages/formulare.aspx abrufbar.

Die Antragsformulare sind an die Benutzer:innen- und Berechtigungsverwaltung zu übermitteln und dort aufzubewahren.

Änderungen an den Formularen können nach Absprache mit der/dem Applikationsverantwortlichen durch die Betriebskoordination vorgenommen werden.